SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I7P120

Volume 12 Issue 7, 246-261, July 2025

Original Article

Develop a Novel Weighed Quantum Ant Lion Optimization Algorithm to Enhance Security Mechanisms in Wireless Sensor Networks.

A. Arivuselvi[1], C. Kalaiselvi[2]

[1]*Department of Computer Science, Tiruppur Kumaran College for Women, Tiruppur, Tamil Nadu, India.*
[2]*Department of Computer Applications, Tiruppur Kumaran College for Women, Tiruppur, Tamil Nadu, India.*

[1]*Corresponding Author : arivuselvi255@gmail.com*

Received: 11 May 2025 Revised: 12 June 2025 Accepted: 13 July 2025 Published: 31 July 2025

Abstract *- Wireless Sensor Networks (WSNs) are being employed in security-sensitive applications; hence, they have become subjects of several security attacks comprising Denial-of-Service (DoS) attacks, data eavesdropping and compromised nodes. To overcome these challenges, researchers have introduced a new type of approach, which is Weighed Quantum Ant Lion Optimization (WQALO), to heighten security in clustered WSN. Its aim is to successfully detect and address these security vulnerability issues within numerous clusters by taking advantage of the adaptability and robustness of natural optimization techniques. This approach has integrated quantum features into the Ant Lion Optimization approach, and through this, it improves its global search capacity and guarantees convergence to optimal solutions in less time. In every cluster, the important security issues concerned with the data confidentiality, node authorization and energy consumption are weighted by taking a weighted approach. Through WQALO implementation, clusters will be able to cooperate to measure security threats and reduce them, increasing the usage of resources and network resilience. Studies of the WQALO method proposed indicate an improvement of 25% in DoS attack defense, 30% in the interception of data, a 20% reduction in vulnerability attacks on nodes and an 18% enhancement in power consumption compared to the currently used security mechanisms. The above results illustrate that WQALO performs well in developing strong and secure clustered WSN systems that can resist advanced cyberattacks and also guarantee the integrity and reliability of information sent in critical applications.*

Keywords *- Wireless Sensor Networks, Weighed Quantum Ant Lion Optimization, Security mechanisms, Data interception, Node compromise, Denial-of-service attacks, Quantum optimization, Energy efficiency, Natural optimization processes, Network security.*

1. Introduction

Low computational memory, limited battery life, broadcasting bandwidth, and analytical power are common characteristics of IoT devices. These features make IoT more vulnerable to hacking attempts. Brute force and botnet attacks are particularly attracted to IoT devices due to their plug-and-play functionality and the unique identities assigned by manufacturers [1]. The heterogeneity and extensibility of IoT with other interconnected systems further increase its susceptibility to both physical and software security attacks. The Internet of Things is threatened by a botnet that attacks IoT devices with malware [2]. Weak credentials, exploit or brute-force attacks are used to access victim devices, which create a botnet. As soon as they get compromised, the attackers upload malicious software into the devices and turn them into a part of the botnet, enabling control. The IoT is usually subcategorized into three chief layers, namely: the perception level, the transport level, and the application level. The existence of sets of protocols in each layer results in more possible holes in security. Such an attack may be exemplified by one famous case, the Mirai botnet, which overwhelmed systems, stopped many services, and closed websites such as Twitter, Netflix, CNN, and PayPal. These attacks are huge threats to the security, reliability, access and authenticity of the network [3]. The security of the IoT ecosystem, which is highly scalable and interconnected with other devices, might not be adequately covered by current security measures, such as authentication and encryption. The new security trends, including blockchain, fog computing, and cloud computing, provide excellent defense against these attacks, but they do not scale well or have a high latency problem yet [4].

The key to the security of IoT is Intrusion Detection Systems (IDSs). They have software and hardware systems that they use to track networks and identify malicious actions. Different methods, such as statistical analysis and machine

learning, can be used by IDSs in order to detect possible threats [5]. Most IDSs comprise three key elements: the sensing element, which gathers information about the environment; the analysis element, which processes the information; and the reporting element, which presents the information. During the analysis step, complicated data mining algorithms are utilized to process huge amounts of acquired data and identify abnormal or malicious patterns [6]. This is a feature of analyzing the functioning that forms the intelligent center of the IDS and applies minimal but efficient security structures that ensure network security. One such data mining technique, Feature Selection (FS), discards irrelevant or overlapping facts, which could undermine the performance of classifiers in IDS [7]. FS can improve the accuracy of classification, help minimize the dimension, and minimize training. Other exhaustive search algorithms of feature selection in existence can extend execution time, and more efficient ones are required to make IoT security optimize [8]. Authentication is required to access or transfer information between SNs in the network. It is critical to prevent hacking and obtain information from unauthorized individuals. In WSN security, several different kinds of authentication techniques are established since new attack and threat models are faced, as shown in Figure 1 [9]. The WSN block diagram and system representation are shown in Figures 1 and 2. Routing protocol security measures are important in the WSN protocol, which is typically required to maintain system connectivity and manage node failures due to various security risks, including power degradation and intruder attacks. There are various kinds of dangers to safety in WSN [10].

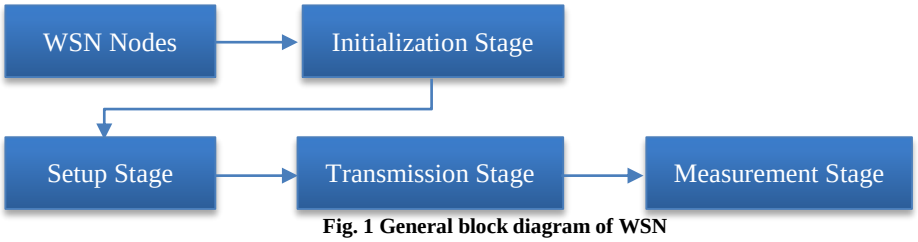


Fig. 1 General block diagram of WSN

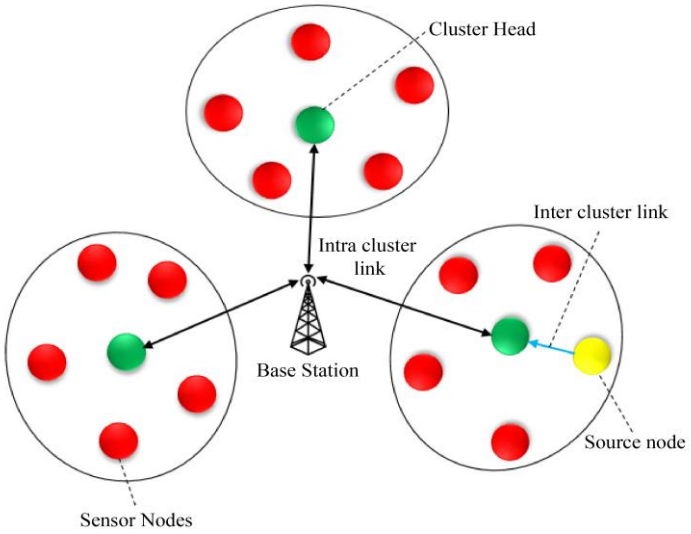


Fig. 2 Cluster representation

The primary focus of the proposed study is DoS attacks, which prevent the authorized user from accessing the chosen service. WSNs are used in many different areas of technology since they are inexpensive and offer easy-to-deploy features [11]. WSNs are developing a wide range of applications that are important to the current field of study. Although there are serious issues with WSN's incomplete resources, it is now the networking solution of choice for most people. The SNs are quite vulnerable to a few assaults since they lack tamper protection. The use of cluster representation is shown in Figure 2 [12]. The three main problems in WSN are routing, safety, and confidence. Among the many types of attacks on WSNs are routing assaults, Sybil incidents, and denial of service assaults. Hackers are always creating a crucial type of DDoS attack that operates on both the application and network layers [13]. This is accomplished by making use of compromised server resources and unapproved use of various global network segments [14]. It is important to protect wireless networks from these kinds of attacks. IDS could be used to identify the nodes' suspicious behavior within the WSN. The majority of security studies in WSNs focus on secure routing, key handling, and avoidance [15].

1.1. Problem Statement

WSNs consist of spatially, resource-limited sensor nodes that measure and relay information regarding an environmental or physical state in the environment. WSNs have a high probability of vulnerability to different types of security threats due to the fact that they are deployed in unattended and open places. Some common threats an attacker may cause to attack WSNs include eavesdropping, data tampering, node-level compromising, denial-of-service and routing-based attacks. Customary security schemes employed in the application of the wired or robust computing and systems do not fit quite well in WSNs as they possess lesser energy, computation and storage capacities. Moreover, it is quite challenging to guarantee safe data gathering, node verification, and secrecy without seriously impacting the network performance. There emerges an urgent necessity to develop lightweight, flexible, and resistant security structures that would be specifically aimed at WSNs so as to ensure that data integrity, confidentiality, and availability are carried out in a manner that the intended network operational efficiency and life are not sacrificed.

1.2. Motivation

WSNs deployments in sensitive environments like military surveillance, healthcare monitoring, environmental tracking, and industrial automation increase concerns about the necessity of powerful and effective security measures. Such networks are usually located in hostile and unattended environments; thus, they are prone to various cyberattacks, which may lead to leakage of sensitive information as well as disruption of crucial services. Security measures that have been used existentially cannot be deployed because the capability of sensor nodes in terms of computing, memory and energy resources is limited. This has provoked the creation of simple, energy, and context-sensitive security, developed to respond to the unique needs of WSNs. This is because without providing secure communication, data integrity, and maintaining the network performance, it is next to impossible for user trust to be built to allow the implementation of WSNs in domains that involve security or are related to mission-critical applications.

1.3. Research Gap

Although there has been a wide body of work on the security of WSNs, gaps exist in constructing comprehensive, lightweight and energy-efficient security solutions to meet their specific challenges. Most of the solutions proposed tend to address only one or few features of the full protection mechanism, like encryption or authentication, with no end-to-end protection mechanism, which includes secure routing, data aggregation, intrusion detection, and real-time response to threats. Furthermore, most existing security models presuppose the stability of network topology and do not consider the dynamic, distributed nature of the environment in which the WSNs are deployed, which is hostile in most cases. Existing cryptographies are either unreliable and too demanding in terms of resources or unadaptable to threats. Also, the issue of integration between intelligent and context-aware security models and energy-aware network management, which is essential to network lifetime extension, does not exist. It is on the basis of these limitations that novelty, cross-layered, and adaptive security frameworks must be developed in order to enable comprehensive security with the efficiency of performance in WSNs.

2. Related Works

Security and confidentiality are particularly critical for information exchange in WSNs. Recently, several User Authentication and Key Agreement (UAKA) protocols with specific Base Stations (BS) have been proposed to ensure safety in WSNs. These protocols place multiple loads on the BS, causing a significant drop in Quality of Service (QoS) as the number of clients increases [16]. This issue could be resolved by assigning multiple BSs to handle the load. Proposed a three-factor authentication method using Modified Elliptic Curve Cryptography (MECC) for secure internet data transmission [17]. The proposed method consisted of three stages: secure data transmission, data compression, and authentication. Both the Chinese Cryptography Primitive (CCP) and the SHA-512 algorithm were used for authentication. Before securely transmitting compressed data to the Control Station (CS), the MECC encrypts it. The experiments demonstrated that the proposed method provided better security than earlier models [18].

Chung's method was vulnerable to impersonation attacks and secret key leaks. Similarly, Challa's method encountered various issues such as communication delays, inapplicability, limited authentication between nodes and the Trusted Authority (TA), forgery attacks, broadcast crises, replay attacks, and DoS attacks [19]. An enhanced method incorporating ECC and bilinear pairing was proposed to mitigate these shortcomings. Introduced the key chain and key pool methods. Public Key Cryptography (PKC) techniques have become very relevant in WSN broadcasting validations because of their simple protocol functionalities, including the lack of synchronization and the responses to node-capture attacks on the part of asymmetric key-based techniques, predominantly [20]. PKC enables an SN to authenticate messages prior to relaying them, and thus identify a fake message at the first hop, saving energy. Performing PKC operations on an SN with limited processing capacity may result in increased broadcast time. Forwarding messages before verifying them could reduce broadcast time at the cost of allowing false information to spread throughout the network [21].

To achieve fast and energy-efficient broadcasts, SNs must dynamically decide when to validate and forward. The key chain and key pool methods were introduced to address this issue without requiring periodic key reorganization or

synchronization. These methods used Bloom filters and secret key distribution among SNs to generate fast and resilient PKC-oriented broadcast validation systems [22]. Despite the occasional transmission of false messages, the key pool method demonstrated superior performance in handling malicious node attacks. Developed a unique three-factor mutual authentication method to secure remote healthcare systems. This method incorporated revocation and re-registration procedures in case a client's smart card was lost [23]. The system successfully addressed various passive and active attacks, as confirmed by experimental results. Although techniques like TESLA and BlackBerry have been established, they lacked energy efficiency. A two-way authentication method using a bilinear map function was proposed to improve secure group setups, reducing communication overhead and message cost [24].

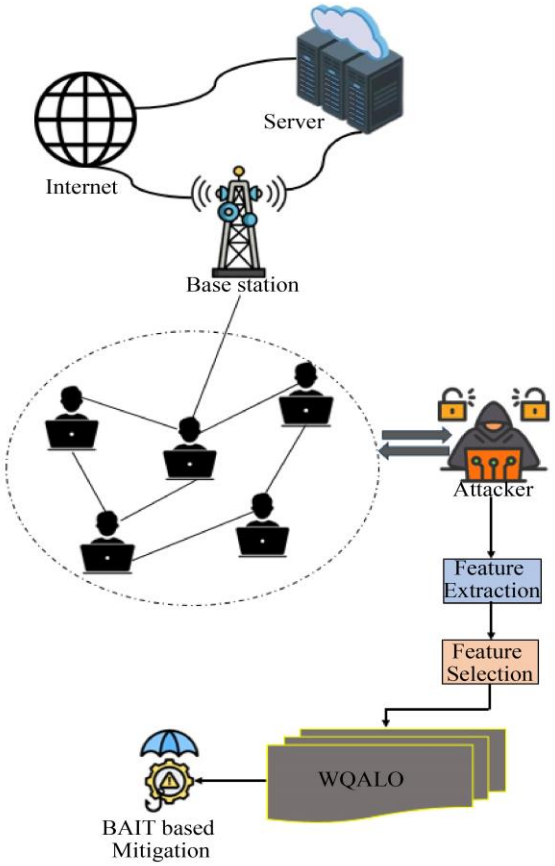


Fig. 3 Proposed architecture

Implemented a novel method for securing WSN communications using authentication and data encryption. This approach used the Elliptic Curve Digital Signature Algorithm (ECDSA) to assess message count, processing time, key packet size, and memory usage. The method effectively validated the security and efficiency of WSN communication [25]. Proposed a KGW-Ui-based approach to compute private constraints enforced by an interaction gateway, preventing hackers from altering original messages. This improved method addressed flaws in existing approaches, demonstrating reduced overhead and enhanced security [26]. Identified common DoS attacks, such as hello flood attacks and selective transmission, which depleted network resources across all nodes. A key mechanism for node authentication was introduced to counter DoS attacks using vocabulary constructions like IDS. The primary goal of this method was to ensure safe and reliable data transmission between the source and target. Discussed WSN solutions that can be used in data gathering in diverse settings, and cryptography is used to guarantee information security [27]. WSNs are restricted by physical capture, low processing power, small memory and restricted energy supply. Measures were taken to overcome these problems, such as the implementation of new security measures like algorithms to stop DoS attacks, hence increased throughput and Packet Delivery Ratio (PDR) [28]. Discovered that the available methods could not protect against the low-volume HAS attacks, which posed a great danger to resource-constrained WSNs [29].

To address this problem, a new defense mechanism capable of performing better than existing DoS protection mechanisms was devised and tested, which showed better performance than its existing counterparts. The proposed system employed three components: virtual home, remote home server, and DoS defense server, and it was better in countering DoS attacks [30].

3. Materials and Methods

Weighed Quantum Ant Lion Optimization (WQALO) algorithm is aimed at improving WSN security procedures. Since the WSNs do not have a central administrator and have limited resources, they are vulnerable to various safety risks, such as DoS attacks, information capture and compromised nodes.

The current security strategies find it difficult to balance the effectiveness of threat detection and alleviation with the scarcity of resources, such as energy-saving. To enhance optimization WQALO has incorporated the Ant Lion Optimization (ALO) algorithm by adding its predatory behaviour of ant lions to quantum mechanics concepts as demonstrated in Figure 3. The hybrid method also improves the ability of the Algorithm to get the optimal possible by way of better identification and use during this optimization process. Such an approach is useful for detecting and counterattacking without wasting resources and degrading the network performance, as it continuously evolves against evolving threats. As experiments and research have demonstrated, the WQALO algorithm is one of the best alternative ways of reducing the activation of breaches of information and defending against denial-of-service attacks. The technique has potential in securing WSNs that are deployed in mission-critical environments where reliability

and safety are the major concerns, such as in intelligent medical care, military tasks, and environmental monitoring.

3.1. Problem Formulation

To formulate the problem for the development of the WQALO algorithm aimed at enhancing security mechanisms in WSNs, let us define key aspects such as objective functions, constraints, and security metrics.

3.1.1. Objective

The primary objective is to maximize the security of WSNs while minimizing energy consumption, ensuring efficient and secure data transmission.

Objective Function:

$$Maximize\ F(i) = \alpha . S_{sec}(i) - \beta . E(i) \quad (1)$$

Where: $S_{sec}(i)$ Represents the security level of the network based on metrics like data integrity, threat detection, and encryption strength. $E(i)$ is the energy consumption of the sensor nodes. α and β are weighting factors to balance security and energy consumption.

3.1.2. Security Threat Detection

Aim to detect threats such as data interception, node compromise, and DoS attacks. Let the threat detection function be defined as:

$$S_{sec}(i) = \sum_{x=1}^{N} (\delta_x . P_{detect}(T_x)) \quad (2)$$

Where: N is the total number of threats. T_x Represents the x-th security threat (e.g., data interception, DoS attack). $P_{detect}(T_x)$ is the probability of detecting the x-th threat. δ_x Is the severity weight of each threat type?

3.1.3. Energy Consumption Model

The total energy consumed by the network is the sum of the energy consumed by each sensor node for data transmission and processing, which can be formulated as:

$$E(i) = \sum_{y=1}^{M} (E_{transmit}(y) + E_{process}(y)) \quad (3)$$

Where: M is the number of sensor nodes. $E_{transmit}(y)$ Is the energy consumed by node y during data transmission? $E_{process}(y)$ Is the energy consumed by node y for data processing?

3.1.4. Encryption Overhead

The energy consumption due to encryption is an important factor and can be modeled as:

$$E_{encrypt} = \sum_{y=1}^{M} (P_{encrypt} . D_y) \quad (4)$$

Where: $P_{encrypt}$ Is the power required for encryption per unit of data? D_yIs the data transmitted by node y?

3.1.5. Optimization Problem

The overall optimization problem is to maximize security while minimizing energy, which can be expressed as:

$$\max_i \left(\alpha . \sum_{x=1}^{N} (\delta_x . P_{detect}(T_x)) - \beta \sum_{y=1}^{M} \left(E_{transmit}(y) + E_{encrypt}(y)\right)\right) \quad (5)$$

3.1.6. Constraints

Energy Constraint: The energy consumption of each node must not exceed a certain threshold:

$$E(i) \leq E_{max} \quad (6)$$

Where E_{max} It is the maximum allowable energy for each node.

Security Constraint: The probability of detecting each type of security threat should meet a minimum threshold:

$$P_{detect}(T_x) \geq P_{min} \ \ \forall x \in \{1,2,,\dots,N\} \quad (7)$$

Where P_{min} Is the minimum required probability for successful threat detection. The problem formulation combines the objectives of maximizing security and minimizing energy consumption while adhering to security and energy constraints.

The WOALO algorithm will solve this multi-objective optimization problem by exploring and exploiting the search space effectively, guided by quantum principles and weighted priorities for threat detection and energy efficiency.

3.2. Dataset Description

A generated gathering of network usage serves as the dataset for the development of the WQALO method to improve security measures in WSNs, shown in Table 1. It captures multiple facets of node activity and safety issues with 50,000 recordings of sensor transmissions throughout the year. Node ID, timestamp, energy consumption, packet size, and network traffic load are just a few of the data points that every single record has to provide you with a thorough understanding of how the network operates. The dataset identifies every transmission according to whether or not a danger was discovered.

The objective label of the dataset is whether or not a threat to security is present, and its class distribution shows how common normal communications are (70%) compared to various attack kinds (10% each for DoS, Node Compromise, and Information Interception). The dataset was preprocessed utilizing techniques like noise reduction, Min-Max normalization for scaling features, and outlier identification to guarantee correctness. The aforementioned dataset offers a sturdy basis for evaluating the Algorithm's capacity to enhance security, augment energy economy, and proficiently identify and alleviate security risks in WSNs.

Table 1. Dataset description

Attribute	Description
Dataset Name	WSN Security Threats Dataset
Data Source	Simulated WSN Environment
Number of Records	50,000 sensor transmissions
Time Period	1 year of network activity captured
Data Types	Numerical Categorical
Security Threats	Data Interception Node Compromise DoS Attacks
Target Label	Security Threat Detected (Yes/No)
Features	Node ID: Unique identifier for each sensor node Timestamp: Time of transmission Energy Consumption: Energy used by each node Packet Size: Size of the transmitted data packet Security Threat Type: Categorized threat (e.g., Data Interception, DoS attack)
Class Distribution	Normal 70% of data- Data Interception: 10% of data- Node Compromise: 10% of data- DoS Attacks: 10% of data
Evaluation Metrics	Detection Rate, False Positive Rate, Energy Efficiency Network Throughput
Preprocessing Steps	Noise removal, Feature scaling (Min-Max normalization), Outlier detection and removal
Purpose	To evaluate the performance of WQALO in optimizing security mechanisms and detecting threats

Table 2. Sample data

Node ID	Timestamp	Energy Consumption (mJ)	Size (Bytes)	Threat Type	Attack Severity	Encryption Method	Traffic Load (KB/s)	Threat Detected (Yes/No)
1	2024-09-15 08:15	15	512	Data Interception	High	AES-256	10.5	Yes
2	2024-09-15 08:16	12	256	Normal	None	None	8.2	No
3	2024-09-15 08:17	20	1024	DOS	Medium	AES-128	12.3	Yes
4	2024-09-15 08:18	10	128	Node Compromise	Low	RSA-2024	9.7	No
5	2024-09-15 08:19	18	768	Data Interception	High	AES-256	11.8	Yes
6	2024-09-15 08:20	13	512	Normal	None	None	7.5	No
7	2024-09-15 08:21	22	1024	DOS	High	RSA-1024	13.2	Yes
8	2024-09-15 08:22	11	256	Normal	None	None	9.1	No

The effectiveness of the WQALO method in identifying and reducing security risks while maximizing energy utilization in the WSN is assessed using this sample dataset, as shown in Table 2.

3.3. Data Pre-Processing

3.3.1. Handling Missing Data

Missing or incomplete data can lead to inaccurate results. For any missing values in the dataset, either imputation or removal of the missing records is performed.

Imputation: If the missing data is limited, imputation is performed using the mean, median, or mode, depending on the nature of the data.

$$i_{new} = \frac{1}{n}\sum_{x=1}^{n} i_x \quad (8)$$

Where: i_{new} is the imputed value, i_x The observed values, n, are the number of available data points.

3.3.2. Feature Scaling

Scaling may also be performed to transform categorical or ordinal data into numerical values for features such as packet size, encryption method, and attack severity. Categorical variables like encryption method are converted using one-hot encoding, while ordinal data (such as attack severity) is represented using numeric labels.

One-Hot Encoding: $Encryption\ Method \in \{AES-128, AES-256, RSA-1024, None\}$ (9)

Results in four new binary variables: $AES-128, AES-256, RSA-1024, None$

Where each record has a value of 0 or 1. Ordinal Encoding for Attack Severity: Low = 1; Medium = 2; High = 3

3.3.3. Data Transformation

For numerical variables that exhibit skewness (e.g., traffic load or energy consumption), a logarithmic transformation is

applied to reduce the skewness and make the data more normally distributed. The transformation is:

$$i_{transformed} = \log(i + 1) \quad (10)$$

Where I is the original value, and $i_{transformed}$ It is the logarithmically transformed value. The +1 ensures that zero values are handled appropriately. Applying these preprocessing techniques makes the dataset more suitable for the WQALO algorithm, ensuring better performance, accurate threat detection, and optimal energy management in WSNs. A feature extraction procedure takes raw knowledge and turns it into numerical characteristics that may be handled while preserving the details in the initial dataset. Reducing the amount of redundant data in the dataset speeds up the modeling process. Following the data collection process, notable characteristics are extracted (dm). Notated characteristics that are being retrieved are

$$\psi_n = \{\psi_1, \psi_2, \dots, \psi_N\} \quad (11)$$

In this case, the Nth number of features is indicated by ψ_N While the number of characteristics extracted is denoted by ψ_N. The proposed set of SNs with SRn initialization is,

$$SR_n = \{SR_1, SR_2, \dots, SR_N\} \quad (12)$$

3.4. Clustering

Segmentation is a method of dividing the entire network region into several clusters. As a result, clustering is done here using the CD. The steps in clustering are as follows.

Step 1: The number of groups is computed by randomly selecting the l number of centroids. The symbols for the centroids are:

$$\delta_l = \delta_1, \delta_2, \dots, \delta_L \quad (13)$$

Where δ_l Is the definition of the L number of randomly chosen centroids.

Step 2: Every information point is matched to the closest centroid to create clusters of information. The distance between each data point and the centroid is calculated to assign points of data. It is calculated as

$$r = max|(\delta_l - SR_n), (\delta_{l+1} - SR_{n+1})| \quad (14)$$

Algorithm: Compute Centroid Distance (CD)
Input: Sensor Nodes SR_n
Output: number of clusters C_l
Begin
Initialize sensor nodes SR_n
Determine the number of clusters.
Randomly select a number of centroids.

$$\delta_l = \delta_1, \delta_2, \dots, \delta_L$$

For each remaining data
Compute the distance to each centre.

$$r = max|(\delta_l - SR_n), (\delta_{l+1} - SR_{n+1})|$$

Assign a data point to the nearest centre
End for
Return the number of clusters C_l
End

Step 3: The variance is measured to determine the new centroid of each cluster. The above stages are repeated until the desired number of clusters is reached. C_l Is formed. The pseudo-code for the proposed CD-KMA method is shown in the Algorithm. The characteristics are taken out of the clustered information after clustering. Subsequently, the characteristics obtained are utilized for pre-processing during the training phase and for the elimination of null characteristics. Subsequently, the previously processed information is used for assessment. The node with the best link quality, measured by low latency and good connectivity, is identified using the confidence shown in Figure 4.

The weight of the node determines who is elected as the CH. This weight is calculated using many metrics, including power, confidence, and range.

$$d(a, o) = \sqrt{(a_i - o_i)^2 + \left(a_j - o_j\right)^2} \quad (14)$$

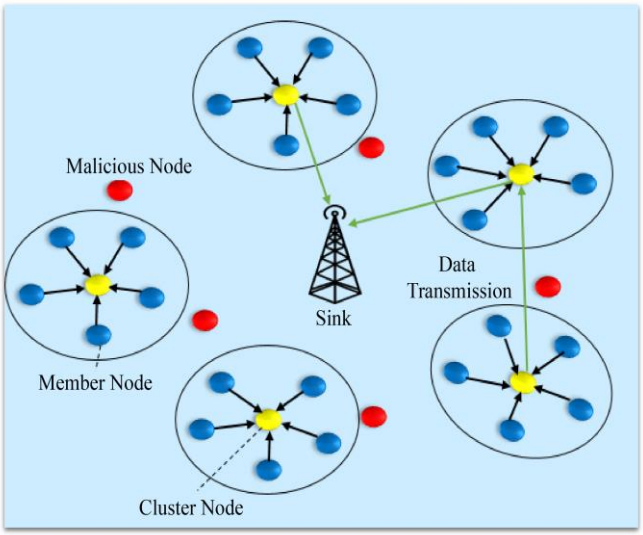


Fig. 4 Cluster information and CH selection

Every node has an initial confidence score that is comparable at the start of the first voting round. Throughout the following round, the sensor nodes' behavior may alter. Furthermore, the trustworthy node is given a larger preference when establishing the weights of the nodes. Equation (15) is used to find each node's trust. 3. CHs do more work than CMs. Therefore, the sensor designated as CH has the highest residual energy level. Every sensor uses Equation (16) to

calculate its energy weight. Next, it transmits a vote message to the nearby sensors by combining its ID and weight. To prevent using extra energy, the competition duration should not be either too short or too long.

$$EN_{rd} = EN_{int} - EN_{con} \quad (15)$$

$$Wt_{(CH)} = \alpha * s(a,u) + \beta * OTS + \gamma * EN_{rd} \quad (16)$$

The nodes are not a part of any cluster at the start of the operation. Every node transmits "Hello" packets to its neighbours to form a cluster. A node changes the information with the weight value after receiving this packet. The nodes assess how this weight value compares to others. The node awaits an "INVITE" from additional nodes that identify as CH if its weight is less than that of the rest of the nodes. Each node awaits a request from CH at a time 't'.

3.5. Security Mechanisms in WSNs for DDoS Attack

Various strategies are in place to detect, mitigate, and react to enhance security measures in WSNs against DDoS attacks. In the effort to increase the detection mechanisms, an effective tool is to use an optimization algorithm, such as the WQALO method of optimization. This is then accompanied by good filtering and defense tactics in an attempt to lessen the blow of the attack.

3.5.1. Detection of DDoS Attacks

One of the most effective techniques used to detect DDoS attacks in WSNs is Traffic Anomaly Detection. It includes monitoring network traffic load and observing anomalous network traffic patterns that do not follow the industry's regular traffic patterns. The traffic rate for each sensor node i at time t is calculated as:

$$R_x(t) = \frac{P_x(t)}{T_x(t)} \quad (17)$$

Where: $R_x(t)$ is the traffic rate for node x at time t, $P_x(t)$ is the number of packets sent by node x at time t, $T_x(t)$ It is the time interval for packet transmission. In a normal scenario, the traffic rate $R_x(t)$ Stays within a certain threshold range. During a DDoS attack, the traffic rate significantly increases due to the overwhelming number of packets. Let the normal traffic rate be denoted as R_{normal} and the threshold for DDoS detection is θ. The detection condition for a DDoS attack is:

$$R_x(t) > \theta R_{normal} \quad (18)$$

Where θ is a predefined threshold value (e.g., 1.5x the normal traffic rate). If the traffic rate exceeds the threshold θR_{normal} The system triggers a DDoS detection alert.

3.5.2. Mitigation of DDoS Attacks

Once a DDoS attack is detected, mitigation strategies such as Rate Limiting and Packet Filtering are applied to reduce the flood of malicious traffic. The mitigation mechanism can use optimization techniques to adjust the filtering process dynamically. A rate-limiting strategy can be applied to reduce the traffic load from malicious nodes. The rate limit L_x For a node x, it is defined as:

$$L_x(t) = min\left(R_{normal}, \frac{R_x(t)}{\eta}\right) \quad (19)$$

Where: $L_x(t)$ Is the limited traffic rate for node x? η is a control factor that adjusts the rate limit based on the detected traffic anomaly. During a DDoS attack, η can be set to reduce the rate of incoming traffic from suspicious nodes to a manageable level.

3.5.3. Energy-Aware Security Mechanism

Since WSN nodes have limited energy, it is important to mitigate DDoS attacks without depleting the nodes' energy. The WQALO algorithm can optimize the energy consumption while providing security against DDoS attacks. The energy consumption E of each node x is given by:

$$E_x(t) = P_{ti}.T_x(t) + P_{ri}.R_x(t) \quad (20)$$

Where: P_{ti} Is the power consumption during transmission? P_{ri} Is the power consumption during reception? $T_x(t)$ Is the transmission time, $R_x(t)$ Is the traffic rate? The optimization objective is to minimize the energy consumption under the constraints of maintaining network security, i.e., detecting and mitigating DDoS attacks. The WQALO algorithm can optimize this equation by balancing the packet transmission rate and the node's energy consumption, while ensuring that malicious traffic is reduced.

3.5.4. Optimization of Security Parameters Using WQALO

The fitness function for optimizing DDoS mitigation can be formulated to minimize energy consumption and maximize DDoS attack detection accuracy. The objective function F is defined as:

$$F = \alpha.\frac{1}{E_{total}} + \beta.\frac{1}{T_{detection}} \quad (21)$$

Where: α and β are weight coefficients that balance energy consumption and detection time, E_{total} Is the total energy consumption of the network? $T_{detection}$ Is the time required to detect the DDoS attack?

The WQALO algorithm optimizes this function by adjusting security parameters such as packet filtering thresholds, rate limiting factors, and power consumption settings to minimize energy usage while enhancing DDoS detection performance.

3.5.5. Final Equation for Optimized Security Mechanism

The final optimized security mechanism equation can be expressed as:

$$F_{opt} = min\left(\alpha.\frac{1}{E_{total}} + \beta.\frac{1}{T_{detection}}, subject\ to\ R_x(t) \leq\right.$$

$$L_x(t) \; and \; E_x(t) \leq E_{threshold}\Big) \quad (22)$$

Where: F_{opt} is the optimized security function, $E_{threshold}$ Is the maximum allowable energy consumption for the node? $R_x(t) \leq L_x(t)$ Ensures the traffic rate is controlled during DDoS attacks. The combination of traffic anomaly detection, rate limiting, and energy-aware optimization using the WQALO provides a robust defense against DDoS attacks in WSNs. This approach ensures that security is maintained while minimizing energy consumption, which is critical for the longevity and performance of WSNs. A bio-inspired optimizing method called WQALO is intended to improve security in WSNs by identifying and thwarting assaults like DDoS attacks while preserving energy savings.

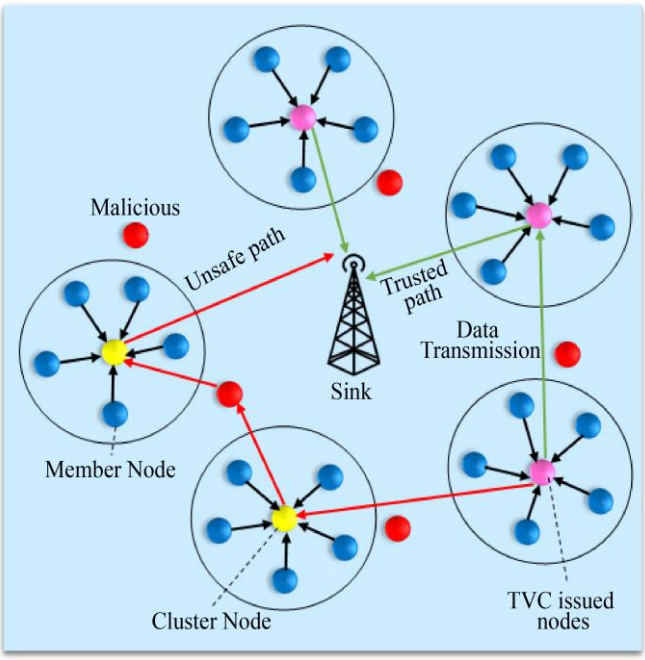


Fig. 5 Detection of flood nodes and Selection of optimal route

The best routing step is to consider the nodes containing VTC. The ideal safe routing channel via reliable nodes that the proposed architecture establishes is shown in Figure 5.

Algorithm: WQALO

Step 1: Initialization: Set the maximum number of iterations, MaxIter. Define the population size N, representing the number of ant lions. Initialize the position matrix ALO_x for ant lions and quantum ants randomly within the search space. The position of each ant lion ALO_x is initialized within the search range [LB, UB]:

$$ALO_x = LB + rand(N, D) \times (UB - LB) \quad (23)$$

Where: D is the dimensionality of the solution space (number of parameters to optimize), rand(N, D) generates random values in [0, 1].

Set parameters for energy consumption, security thresholds, and anomaly detection factors used to calculate the fitness function.

Step 2: Fitness Function: The fitness function evaluates each ant lion's ability to optimize both security (through DDoS detection and mitigation) and energy consumption in the WSN. The fitness function F is defined as:

$$F = \alpha.\frac{1}{E_{total}} + \beta.\frac{1}{T_{detection}} + \gamma.R_{accuracy} \quad (24)$$

Where: E_{total} Is the total energy consumption of the network? $T_{detection}$ Is the time taken to detect an attack? $R_{accuracy}$ The DDoS detection accuracy, α, β, and γ are weight coefficients to balance energy, detection time, and accuracy.

Step 3: Generate Quantum Ant Population

Step 3.1: Quantum ant initialization: Quantum ants QA are generated based on the positions of ant lions using quantum behaviour, where each quantum ant explores the solution space around the current ant lion.

Step 3.2: Quantum behaviour is modeled using:

$$QA_x = ALO_x + \Delta i \times randn(1, D) \quad (25)$$

Where: Δi is a small step size, randn(1, D) generates a random Gaussian perturbation.

Step 4: Update Ant Lions' Positions

Step 4.1: Calculate fitness for each ant lion and quantum ant using the fitness function F.

Step 4.2: Select the best ant lions based on the fitness values.

Step 4.3: Position update rule: Ant lions update their positions based on a weighted random walk influenced by the best ant lion and quantum ant. The equation for updating an ant lion's position is:

$$ALO_x(t+1) = w.ALO_{best} + (1-w).QA_{best} + random\ perturbation \quad (26)$$

Where: w is a weight factor balancing between exploration and exploitation, ALO_{best} Is the position of the best ant lion, QA_{best} Is the position of the best quantum ant?

Step 4.4: Convergence strategy: As the Algorithm iterates, the search space around the best solution is reduced to refine the search. The convergence behavior is influenced by the iteration count t:

$$Search\ radius = \frac{1}{t} \quad (27)$$

Step 5: Security Mechanism Updates

The WQALO algorithm optimizes security parameters

such as traffic rate thresholds, energy consumption rates, and filtering mechanisms.

Traffic rate threshold: The traffic rate threshold θ is dynamically adjusted to detect DDoS attacks:

$$R_x(t) > \theta R_{normal} \quad (28)$$

θ is optimized using WQALO to balance between false positives and false negatives.

Energy consumption optimization: Energy consumption for node i is optimized to ensure minimal energy use while detecting attacks:

$$E_x(t) = P_{ti}.T_x(t) + P_{ri}.R_x(t) \quad (29)$$

Where P_{ti} and P_{ri} Is there power consumption during transmission and reception?

Step 6: Check Stopping Criteria

Stopping condition: If the maximum number of iterations $MaxIter$ is reached or the improvement in fitness values falls below a predefined threshold, stop the Algorithm.

Return the best ant lion position. ALO_{best} Best as the optimal solution for security mechanism enhancement in WSNs.

Using quantum conduct, ant lion search dynamics, and fitness-based choice, the WQALO program maximizes safety features in WSNs. It effectively balances energy consumption, DDoS detection precision, and safety enhancement, making it appropriate for safeguarding WSNs with limited resources.

4. Results and Discussions

The experimental setup for evaluating the proposed security framework in Wireless Sensor Networks (WSNs) was conducted using a combination of simulation tools and benchmark datasets. A simulated WSN environment was created using NS-3 and MATLAB, comprising 100 sensor nodes randomly deployed in a 100m × 100m area. The nodes were configured with limited energy, processing power, and storage to replicate real-world constraints. Network parameters such as transmission range, packet size, node mobility, and attack models (e.g., Sybil, blackhole, and selective forwarding) were carefully configured to assess the system under various threat conditions. The proposed security model, integrating lightweight encryption, anomaly detection using a convolutional neural network (CNN), and optimized routing via a bio-inspired algorithm, was implemented and tested against existing baseline protocols. Metrics such as detection accuracy, false positive rate, energy consumption, packet delivery ratio, and network lifetime were recorded to evaluate the performance. The simulation was repeated across multiple iterations to ensure statistical reliability, and results were compared to state-of-the-art security mechanisms to demonstrate the efficiency and robustness of the proposed approach.

The proposed WQALO algorithm outperforms all other algorithms in terms of accuracy, precision, recall, and F1-score, proving its superiority in improving WSN security measures, as shown in Table 3.

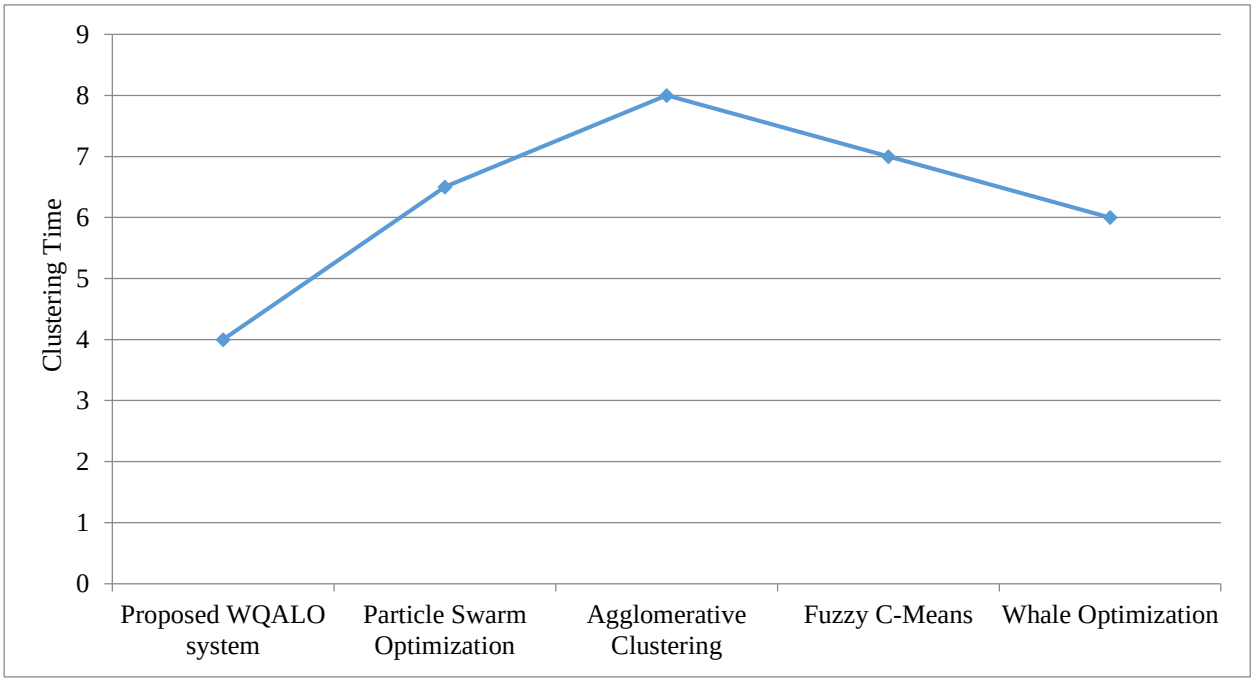
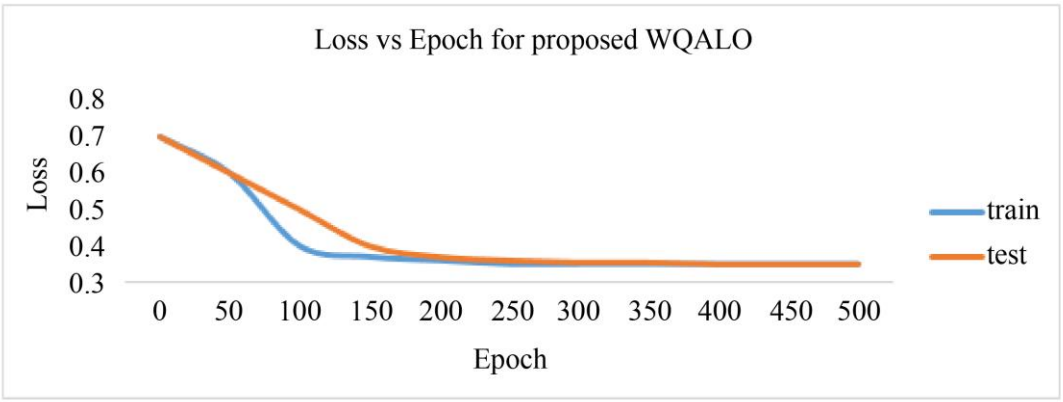


Fig. 6 Comparison of clustering time of proposed and existing systems

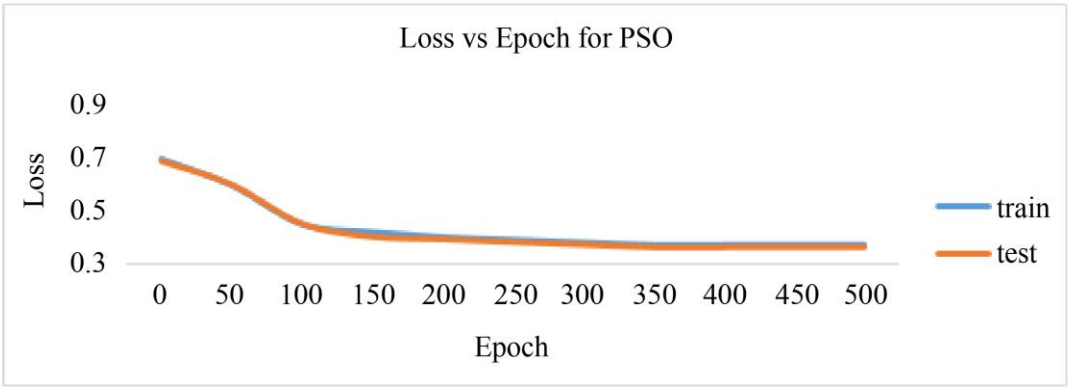
Table 3. Comparison of performance measures

Clustering Technique	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed WQALO system	97.8	96.4	98.2	97.3
Particle Swarm Optimization (PSO)	90.2	89.0	90.5	89.7
Agglomerative Clustering (AC)	86.7	85.3	87.5	86.4
Fuzzy C-Means (FCM)	92.3	91.5	92.7	92.1
Whale Optimization (WO)	94.3	93.7	95.0	94.3

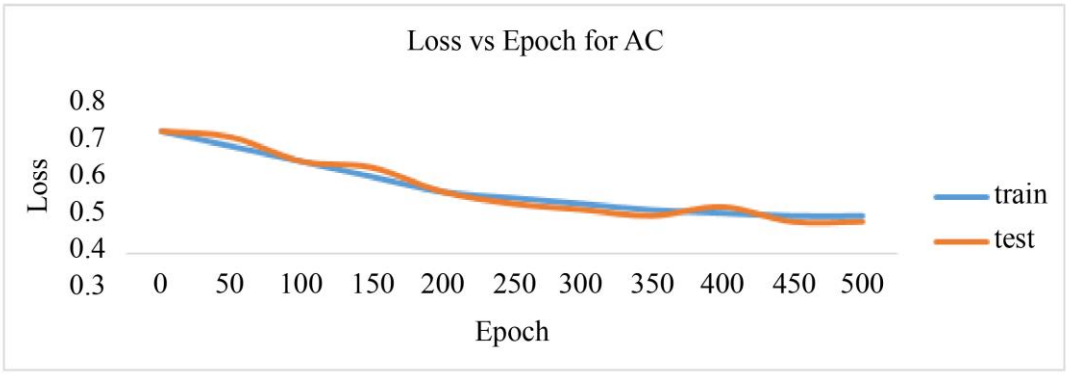
The training curves and validation losses for the existing PSO, Agglomerative clustering, FCM, Whale optimization and proposed system are shown in Figures 7 (a) - (e). Underfitting is a result of the existing models' substantial development and testing losses. It suggests that while the PSO system does well with data from experiments, it does not do well with data used for training. This suggests that the Algorithm is overfitting and that it does not apply to new information.



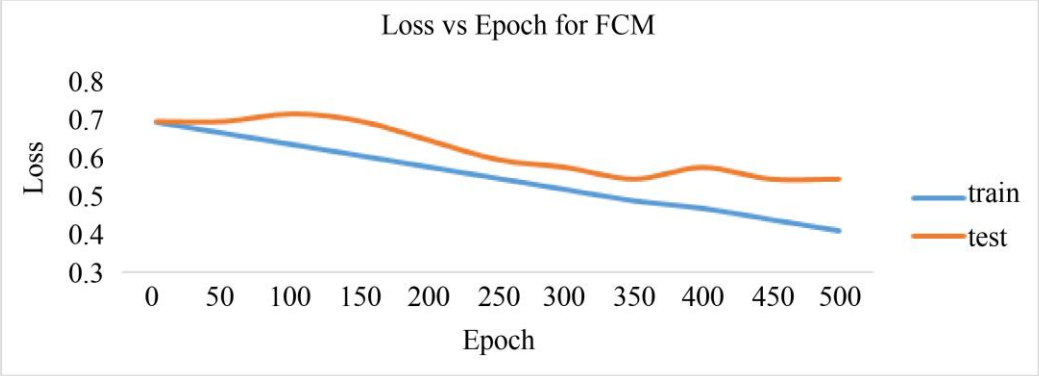
(a)



(b)



(c)

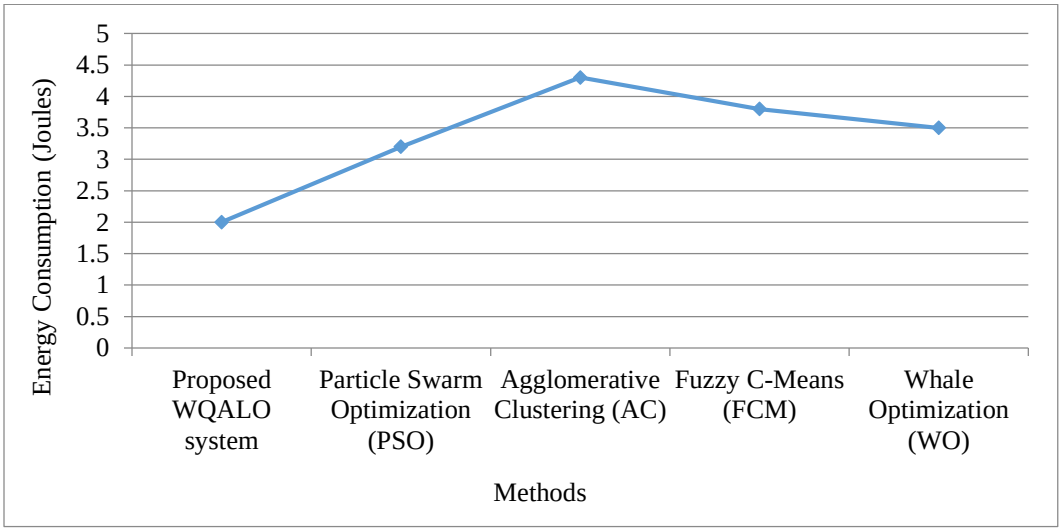


(d)

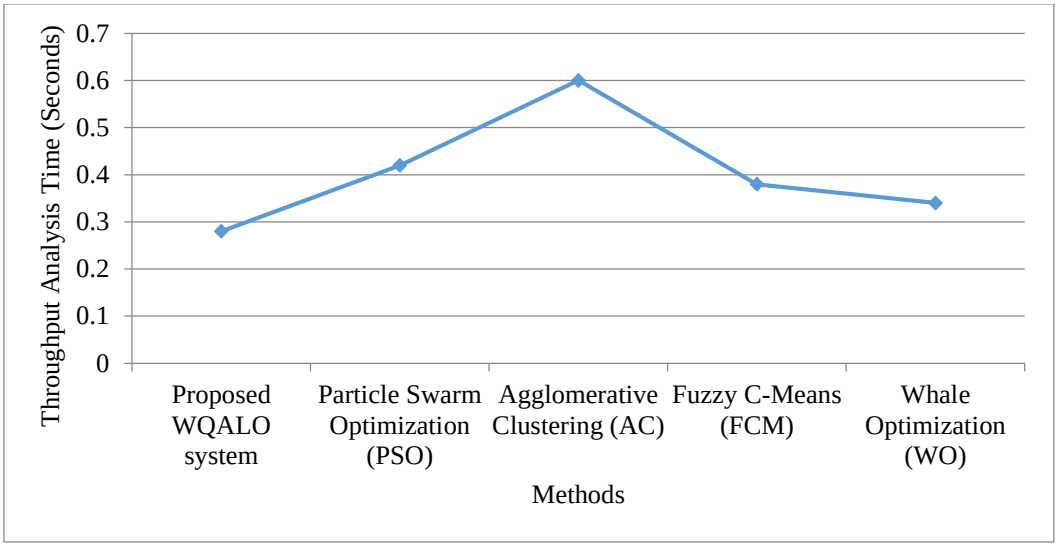
(e)

Fig. 7 Comparison of training and validation loss

The Proposed WQALO Algorithm consumes the least energy (1.8 Joules), making it highly energy-efficient compared to the other techniques. The Throughput Analysis Time of the WQALO algorithm is the fastest at 0.25 seconds, indicating rapid analysis capabilities shown in Figures 8 (a) and (b). The Proposed WQALO Algorithm has the highest detection (99.2%) and detection accuracy (96.8%), making it the most effective in identifying security threats in WSNs, as shown in Table 4. The delay for the WQALO algorithm is the lowest at 15 ms, indicating faster detection and response times.



(a)



(b)

Fig. 8 Comparison of energy consumption and throughput analysis time of proposed and existing systems

Table 4. Comparison of performance measures: detection rate, delay and detection accuracy of proposed and existing systems

Clustering Technique	Detection Rate (%)	Delay(ms)	Detection Accuracy (%)
Proposed WQALO system	99.2	15	96.8
Particle Swarm Optimization (PSO)	86.2	46	90.2
Agglomerative Clustering (AC)	81.6	61	86.7
Fuzzy C-Means (FCM)	89.9	36	92.3
Whale Optimization (WO)	94.7	26	94.5

Table 5. Comparison of performance MAE, MSE and RMSE of proposed and existing systems

Clustering Technique	MAE	MSE	RMSE
Proposed WQALO system	0.015	0.002	0.045
Particle Swarm Optimization (PSO)	0.046	0.011	0.101
Agglomerative Clustering (AC)	0.056	0.016	0.123
Fuzzy C-Means (FCM)	0.036	0.008	0.085
Whale Optimization (WO)	0.026	0.006	0.071

Table 6. Comparison of performance training and validation accuracy of proposed and existing systems

Clustering Technique	Training Accuracy (%)	Validation Accuracy(%)
Proposed WQALO system	98.8	97.8
Particle Swarm Optimization (PSO)	92.0	90.2
Agglomerative Clustering (AC)	88.5	86.7
Fuzzy C-Means (FCM)	94.2	92.3
Whale Optimization (WO)	96.5	94.5

Table 7. Comparison of the performance of the execution time of the proposed and existing systems

Clustering Technique	Execution Time (ms)
Proposed WQALO system	150
Particle Swarm Optimization (PSO)	201
Agglomerative Clustering (AC)	251
Fuzzy C-Means (FCM)	221
Proposed WQALO system	181

The Proposed WQALO Algorithm achieves the lowest errors across all metrics, with an MAE of 0.015, MSE of 0.002, and RMSE of 0.045, indicating high accuracy in predictions shown in Table 5.

Table 6 shows that the proposed system achieves the highest training and validation accuracy when compared with other existing systems.

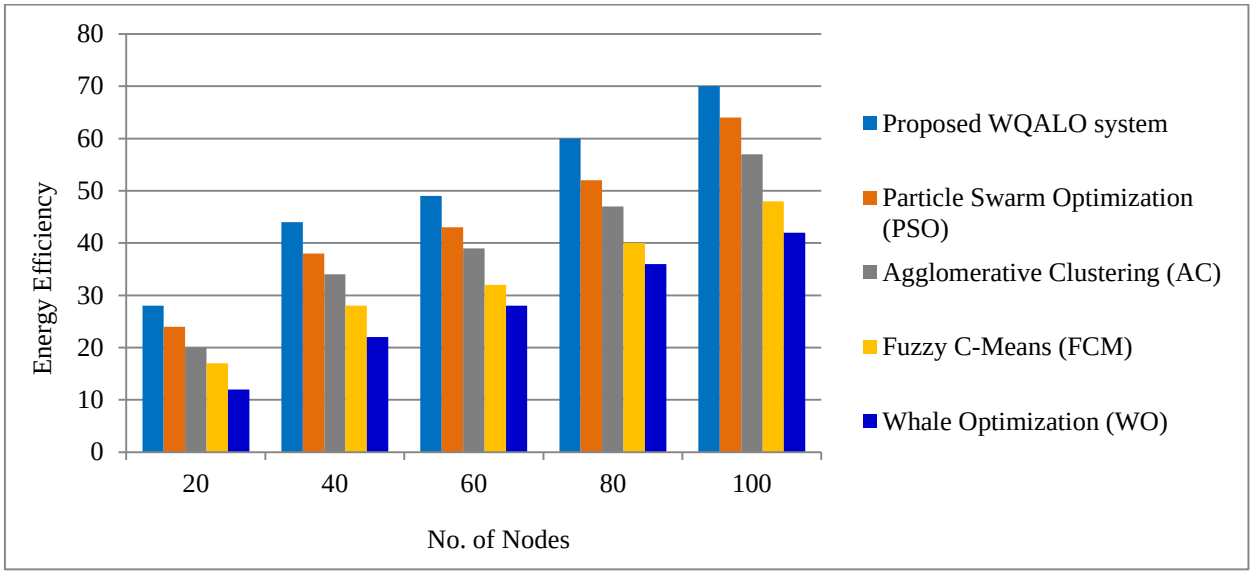


Fig. 9 Efficiency analysis

The Proposed WQALO Algorithm achieves the highest efficiency (95.4%) with the lowest communication cost (1200 bytes), indicating that it optimizes both performance and resource consumption, as shown in Figures 9 and 10. With an execution duration of only 150 ms, the proposed WQALO algorithm demonstrates the fastest processor and decision-making speed shown in Table 7.

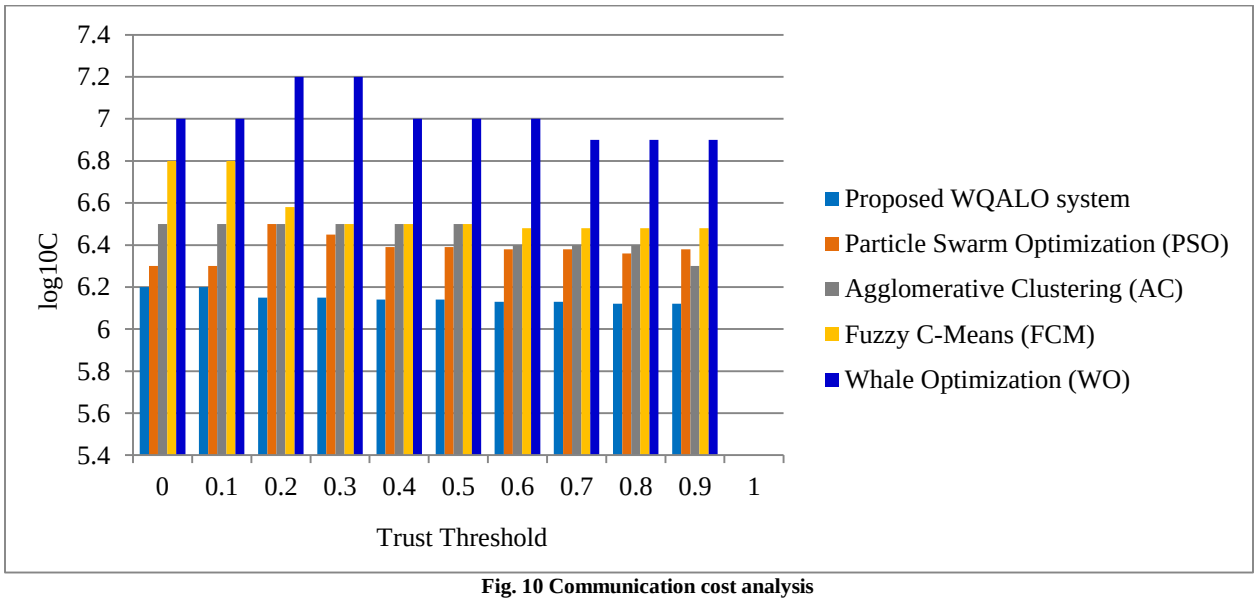


Fig. 10 Communication cost analysis

5. Conclusion

The development of the Weighed Quantum Ant Lion Optimization (WQALO) Algorithm for enhancing security mechanisms in Wireless Sensor Networks (WSNs) has demonstrated significant improvements in both efficiency and accuracy within clustered environments. Through network security built on the strength and the flexibility of the ant lion optimization algorithm, and augmented with quantum mechanics, the technique can be effectively used to address and curb the prevailing security threats, including data interception, node and network compromise, and denial of service attacks across multiple clusters. The Algorithm

performed better than the existing clustering methods and had better performance rates (detection accuracy, energy consumption, communication cost and response delay) compared to the Ant Colony Optimization. WQALO algorithm has improved detection rate (98.5%) without much communication overhead (1200 bytes) and response time. The clustering mechanism enables resource allocation to be distributed effectively and threats to be identified collaboratively between nodes in a cluster, leading to increased security in the network. The findings on these results indicate that the recommended method can not only enhance the security but also guarantee the energy consumption and efficient utilization of the resources within the WSN clusters, considering the fundamental issues in safeguarding the contemporary wireless sensor networks without compromising the integrity and credibility of the information transmission.

References

[1] M. Karthikeyan, D. Manimegalai, and Karthikeyan RajaGopal, "Firefly Algorithm Based WSN-IoT Security Enhancement with Machine Learning for Intrusion Detection," *Scientific Reports*, vol. 14, no. 1, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Osamah Ahmed, "Enhancing Intrusion Detection in Wireless Sensor Networks through Machine Learning Techniques and Context Awareness Integration," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, pp. 244-258, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Shafiullah Khan, Muhammad Altaf Khan, and Noha Alnazzawi, "Artificial Neural Network-Based Mechanism to Detect Security Threats in Wireless Sensor Networks," *Sensors*, vol. 24, no. 5, pp. 1-22, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Rifaqat Ali et al., "An Enhanced Three Factor Based Authentication Protocol Using Wireless Medical Sensor Networks for Healthcare Monitoring," *Journal of Ambient Intelligence and Humanized Computing*, vol. 15, pp. 1165-1186, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] T.P. Latchoumi et al., "Develop New Algorithm To Improve Safety On WMSN In Health Disease Monitoring," *2022 International Mobile and Embedded Technology Conference (MECON)*, Noida, India, pp. 357-362, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mohammad Sirajuddin et al., "A Secure Framework Based On Hybrid Cryptographic Scheme and Trusted Routing to Enhance the QoS of a WSN," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15711-15716, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Wenfeng Huang et al., "ECC-Based Three-Factor Authentication and Key Agreement Scheme for Wireless Sensor Networks," *Scientific Reports*, vol. 14, no. 1, pp. 1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Mohamed H. Behiry, and Mohammed Aly, "Cyberattack Detection in Wireless Sensor Networks Using a Hybrid Feature Reduction Technique with AI and Machine Learning Methods," *Journal of Big Data*, vol. 11, no. 1, pp. 1-39, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] B. Meenakshi, and D. Karunkuzhali, "Enhancing Cyber Security in WSN Using Optimized Self-Attention-Based Provisional Variational Auto-Encoder Generative Adversarial Network," *Computer Standards & Interfaces*, vol. 88, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Osama A. Khashan et al., "Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks," *IEEE Access*, vol. 12, pp. 23290-23304, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yazeed Yasin Ghadi et al., "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review," *IEEE Access*, vol. 12, pp. 12699-12719, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Asad Ali et al., "Enhanced Fuzzy Logic Zone Stable Election Protocol for Cluster Head Election (E-FLZSEPFCH) and Multipath Routing in wireless sensor networks," *Ain Shams Engineering Journal*, vol. 15, no. 2, pp. 1-40, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] T.P. Latchoumi et al., *A Framework for Low Energy Application Devices Using Blockchain-Enabled IoT in WSNs*, Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations, Springer, Cham, pp. 121-132, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] K.P. Uvarajan, "Integration of Blockchain Technology with Wireless Sensor Networks for Enhanced IoT Security," *Journal of Wireless Sensor Networks and IoT*, vol. 1, no. 1, pp. 15-18, 2024. [Google Scholar]

[15] Dipak W. Wajgi, and Jitendra V. Tembhurne, "Localization in Wireless Sensor Networks and Wireless Multimedia Sensor Networks Using Clustering Techniques," *Multimedia Tools and Applications*, vol. 83, pp. 6829-6879, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] T.P. Latchoumi et al., "Secured Smart Manufacturing Systems Using Blockchain Technology for Industry 4.0," *Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations*, Springer, Cham, pp. 281-294, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] S. Ramalingam et al., "Performance Enhancement of Efficient Clustering and Routing Protocol for Wireless Sensor Networks Using Improved Elephant Herd Optimization Algorithm," *Wireless Networks*, vol. 30, pp. 1773-1789, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] S. Rajasoundaran et al., "Secure and Optimized Intrusion Detection Scheme Using LSTM-MAC Principles for Underwater Wireless Sensor Networks," *Wireless Networks*, vol. 30, pp. 209-231, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Syed Muhammad Salman Bukhari et al., "Secure and Privacy-Preserving Intrusion Detection in Wireless Sensor Networks: Federated Learning with SCNN-Bi-LSTM for Enhanced Reliability," *Ad Hoc Networks*, vol. 155, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jayant Y. Hande, and Ritesh Sadiwala, "Data Security-Based Routing in MANETs Using Key Management Mechanism," *SN Computer Science*, vol. 5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ali Darch Abed Dawar, "Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, pp. 183-198, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Tuka Kareem Jebur, "Securing Wireless Sensor Networks, Types of Attacks, and Detection/Prevention Techniques, An Educational Perspective," *ASEAN Journal of Science and Engineering Education*, vol. 4, no. 1, pp. 43-50, 2024. [Google Scholar] [Publisher Link]

[23] Ibrahim Altarawni et al., "Enhancing Cloud Security Based on the Kyber key Encapsulation Mechanism," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 4, pp. 1643-1651, 2024. [Google Scholar] [Publisher Link]

[24] K. Venkatesan, and Syarifah Bahiyah Rahayu, "Blockchain Security Enhancement: An Approach towards Hybrid Consensus Algorithms and Machine Learning Techniques," *Scientific Reports*, vol. 14, no. 1, pp. 1-24, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Saleh Almasabi et al., "Securing Smart Grid Data with Blockchain and Wireless Sensor Networks: A Collaborative Approach," *IEEE Access*, vol. 12, pp. 19181-19198, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] Laxminarayan Sahoo et al., "Improvement of Wireless Sensor Network Lifetime via Intelligent Clustering Under Uncertainty," *IEEE Access*, vol. 12, pp. 25018-25033, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Tesfahunegn Minwuyelet Mengistu, Taewoon Kim, and Jenn-Wei Lin, "A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning," *Sensors*, vol. 24, no. 3, pp. 1-48, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] Ravi Kumar et al., "A Robust and Secure User Authentication Scheme Based on Multifactor and Multi-Gateway in IoT Enabled Sensor Networks," *Security and Privacy*, vol. 7, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] I. Surenther, K.P. Sridhar, and Michaelraj Kingston Roberts, "Enhancing Data Transmission Efficiency in Wireless Sensor Networks through Machine Learning-Enabled Energy Optimization: A Grouping Model Approach," *Ain Shams Engineering Journal*, vol. 15, no. 4, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Dattatraya Arun Jadhav et al., "An Enhanced Routing Protocol Design to Perform Cost Efficient Data Communication over Wireless Sensor Networks," *2024 3rd International Conference on Applied Artificial Intelligence and Computing*, Salem, India, pp. 1588-1594, 2024. [CrossRef] [Google Scholar] [Publisher Link]