Yugoslav Journal of Operations Research
34 (2024), Number 4, 725-742
DOI: https://doi.org/10.2298/YJOR240215023Y

AN IMPROVED SUNFLOWER OPTIMIZATION ALGORITHM FOR CLUSTER SELECTION WITH SECURED DATA TRANSMISSION USING CRYPTOGRAPHIC TECHNIQUES IN WSNS -IOT

Dr. Yuvaraja M*

Associate Professor, Department of ECE, P. A. College of Engineering and Technology, Pollachi-642001, yuvarajmuthusamy@gmail.com

Sureshkumar S

Assistant Professor, Department of Computer Science and Engineering, P. A. College of Engineering and Technology, Pollachi-642001, sureshkumar.pacet@gmail.com

Joseph James S

Assistant Professor, Computational Intelligence , College of Engineering & Technology, SRM Institute of Science and Technology, Chennai, Tamil Nadu, josephjs@srmist.edu.in

Ishwarya Niranjana M

Assistant Professor, Department of ECE, Sri Eshwar College of Engineering, Coimbatore. 641202, ishu.niranjana@gmail.com

Received: February 2024 / Accepted: June 2024

Abstract: Security and energy consumption are the two greatest issues of wireless sensor networks. Large numbers of malicious nodes might be found in sensing equipment. To find these rogue nodes, the researchers have proposed a number of strategies. The data must be protected from avoid attacks on these networks and data transfers.This project aims to enable secure routing and mutual authentication via an IoT-based WSN.This study presents a unique algorithm for selecting the top CHs in IoT-WSN. The new technique is an Improved Sunflower Optimisation technique (ISFO), which combines the Levy Flight Operator. The functions of the suggested method can be regulated by such invocation. The suggested method can avoid becoming stuck in local minima by balancing the processes of diversification and intensification. The application of cryptography techniques helps provide reliable and effective solutions to security needs. Nowadays, key management is utilized mostly for data secrecy to provide trustworthy security systems and give an overview of the cryptographic techniques used to clarify

* Corresponding author

security concerns with wireless sensor networks. The proposed ISFO protocol offers consistent results in for end-to-end delays (E2E_Delay), network throughputs (NT), packet delivery ratios (PDR), and network lifetimes during performance evaluations. The proposed protocol beat all other earlier research by offering WSN hybrid security, optimized coverage, and energy efficiency.

Keywords: Wireless sensor network (WSNs), sunflower optimization algorithm (SOA), improved sunflower optimization algorithm (ISFO), cryptography.

MSC: 94Axx, 94A60, 68W40, 90C59, 68T05.

1. INTRODUCTION

Many applications employ wireless sensors which have constraints in memory, battery, bandwidths, and unreliable transmissions. Data processing and storage for wireless sensor networks (WSN) are lab or labour-intensive tasks [1]. Consequently, data requiring independent processing are stored in sensor network, while other data are stored for later use in WSNs [2]. The Internet of Things is specifically utilized for target tracking, fall detection, leak detection, and intrusion detection [3]. Numerous nodes are positioned across the IoT paradigm, and each one performs sensing, processing, and monitoring functions depending on coverage and connection [4].

Dynamic WSNs, as opposed to their static versions allow for the mobility of sensor nodes, which facilitates a more focused and accurate administration [5]. Due to limited IoT resources, uploading acquired data straight to clouds cause power drainage and network shut downs [6]. The acquired data must be sent to a different base station (BS) close to the sensor nodes to address this problem, and these BSs must subsequently transport the data to the cloud. Symmetric encryption-based dynamic WSN encryption key management protocols have already been proposed [7] to address security concerns.

Conventional approaches to WSN security mainly address data transmission security at the network layer, ignoring the essential problem of detecting and reducing the impact of adversarial nodes in the network. Data corruption, network congestion, and service interruption are among the outcomes that might result from adverse nodes engaging in data injection, manipulation, or node compromise, all of which threaten the integrity and dependability of WSNs. Traditional intrusion prevention systems often use signature-based or anomaly detection methods, which may fail to identify complex attacks or zero-day vulnerabilities. Regarding WSNs with limited resources, these procedures are not viable because of the considerable communication and processing overhead they often impose.

To solve these issues, a new method, the upgraded Sunflower optimization method for CH selection and secure data transmission, was developed to increase the nodes' lifespan while decreasing their energy consumption. The proposed method makes advantage of the lèvy flight operator to extend the life of a sensor network and prevent being in local minima. This study's data collection has been improved while keeping a high degree of security. The infrastructure lasts longer since less energy is used. The trials' findings show that the strategy reduces end-to-end latencies, PDR, network longevity, and throughputs. One stochastic search mechanism that takes its signals from Levy flights random walks with significant advances every so then is the Levy Flight Operator. In optimization algorithms, Levy flights enable long-distance explorations of search spaces and allow algorithms to escape local optimas while identifying promising

areas more effectively. Levy flights allow ISFO to explore the search space more thoroughly, especially in distant or undersampled areas. This improves the algorithm's ability to find optimum or near-optimal solutions, particularly in complicated or high-dimensional optimization landscapes, and to successfully overcome local optima.To begin, ISFO provides a one-of-a-kind blend of optimization and security properties developed for use in WSNs-IoT scenarios. While most clustering algorithms aim to maximize network coverage or minimize energy usage, ISFO uses cryptographic methods to ensure data is sent securely across the network. By directly incorporating encryption, key management, authentication, and integrity protection techniques into the optimization process, ISFO delivers a comprehensive solution that concurrently solves both clustering efficiency and data security needs. Simplifying the design and deployment of safe WSNs-IoT systems, this integrated method guarantees that security concerns are intrinsically entrenched in the clustering process.

2. LITERATURE REVIEW

Nabavi et al. [8] used gravitational search techniques to suggest a unique optimization approach for assembling wireless sensor network clusters. Cluster heads (CHs) are chosen using multi-objective genetic algorithm based on reducing intra-cluster ranges, energies used by nodes, and data is transferred amongst netween CHs and sink nodes. The implementation findings demonstrate that the suggested approach functions better than current methods concerning energy usages, data transmission rates, productivity, and data packet transfer rates. Lin et al. [9] developed PM-K-Means, k-means optimized clusters based on particle swarm optimization and multiclass merging. The approach optimized clusters and refining particle swarms clusteris with default counts of clusters. Subsequently, clusters are merged based on multiclass merges for optimal results. The results of the experiments show that the method, with a quicker convergence rate, better global search capabilities, and an enhanced cluster category effect, may effectively overcome the shortcomings of K-means.

Yang et al. [10] Levy Flight Butterfly Optimisation Algorithm-based new algorithm for selection of CHs has been proposed. The levy combat operator is first developed to enhance the BOA's search capabilities. The developed fitness function selecting CHs use node residual energies and distances. The better cluster head is thoroughly chosen using the upgraded BOA, which enhances the random problem of selection of CHs. The approach carefully takes into account variables like node energy and distance. The modelling results, in contrast, show that they have a better impact on longevity and energy consumption.Patil [11]. For CWSNs, two safe, secure, and effective data transmission (SET) protocols have been put forth: the Identity-Based Online/Offline Digital Signature (IBOOS) strategy and the Identity-Based Digital Signature (IBS) method. LEACH (Low-Energy Adaptive Clustering Hierarchy) is a cluster routing scheme that is examined and improved. Resolving the Diffie-Hellman challenge is necessary to secure SET-IBS in the paired domain.Although the stability of the discrete logarithm issue is necessary for its defence, ET-IBOOS also lowers the operational cost, which is essential for WSNs. By balancing the network's energy consumption, our Enhanced LEACH clustering routing system expands on the LEACH protocol.According to the simulation results, they have enhanced LEACH, which beats network system longevity and energy consumption reduction.

Deena Sivakumar et al. [12] introduced the energy-aware clustering protocol utilizing a chaotic gorilla troops optimization algorithm (EACP-CGTOA) for WSN. The CGTOA improves the optimization algorithm's overall performance and diversifies the population. The EACP-CGTOA model uses three input parameters: the energy ratio (ER), the distance to the base station (DBS), and the distance to the neighbours (DTN) to create a fitness function. Several simulations were run to guarantee the improved efficiency of the EACP-CGTOA method, and their results were evaluated from multiple angles. The experimental findings confirmed that the EACP-CGTOA model significantly outperforms current techniques in terms of both network longevity and energy efficiency.

Selvarajan Shitharth et al. [13] presented Federated learning optimizations with analyses of offloads for blockchain computations and enhanced security. Integrating an offloading mechanism for data processing using blockchain technology, where total security is maintained for each data, is the primary relevance of the suggested method. Data weights to balance loads along with parametric assessments performed in real-time to ascertain consistency of data monitored with IoT, is a result of problem approachs built concerning clusters. Results that were investigated using a five-scenario procedure show that offloading analysis with blockchain is safer, leading to 89% more accurate data processing for all IoT applications.

Vanita Verma and Vijay Kumar Jha [14] proposed Mutation grounded Multi-Layer Perceptron (MUMLP) for secure energy aware optimal routes in data transmissions and reduce transmission times. Best CHs are found using Boltzmann Selection Probability-centric Gravitational Search Algorithm (BSP-GSA) for Data Aggregation (DA). After the network's nodes are initialized, several tasks are carried out. Then, the non-cluster members are joined with a neighbouring CH to create a cluster. The CHs collect the data like non-cluster members do; moreover, the collected data is encrypted using the Improved Elliptical Curve Cryptography (IECC) technique, which enhances data security. The encrypted data is sent to the Base Station (BS) via the best path determined by a Deep Learning (DL) algorithm (MUMLP) that takes into account a new fitness function. A cloud server stores the data in the BS for user access. The BlockChain (BC)-enabled authentication is used to avoid unwanted access. According to the results, the algorithm ensures secure and energy-aware data transfer compared to the current methods.

Seyyed Esmaeil Najaf et al. [15] investigated factors impacting sustainment marketing based on IoT. Achieving an extended competitive edge for the company may be achieved with the help of the IoT and the possibilities it offers to managers. Studies have shown that the following factors significantly impact the adoption of the IoT in long-term smart marketing: perceived utility, reliability, ease of use, social acceptability, and controllability. We analyzed and prioritized these crucial indicators in our analysis. Lastly, a structure is provided for articulating the viewpoints on how the IoT affects environmentally aware marketing.

Mali Shrikant Deelip and Govinda Kannayaram [16] suggested exponential-sunflower optimizations and deep convolution neural networks for secure routing and predictions in IoT. Fitnesses were computed by considering trust factors, energies, and distances. When determining the level of trust between two nodes, many factors are considered, including direct, suggested and historical trusts with availability rates. The sensed data collected at the sink node is used when classifying leaf illnesses. The Adam approach trains a deep convolution neural network (DCNN), which is then used to

classify leaf diseases. The suggested Exponential-SFO has a high energy output of 0.420 J, a low latency of 0.0003 s, a high throughput of 7533.75 kbps, and a high accuracy of 94.5%.

To be more specific, existing WSNs-IoT clustering algorithms often fail to consider the vital component of network security while processing data, instead depending on unrelated security protocols or procedures. When security concerns are not addressed explicitly during cluster setup and operation, the resulting solutions may be poor, and the network may be vulnerable.

3. PROBLEM DEFINITION

The research attempts to optimize energy utilizations as energies are precious resources in IoT and enhance IoT network's lifespan [17]. The CHs in the IoT network can be selected with minimal energy by employing clustering techniques and thus consequently, extend network's operating lifespan. Key exchange and digital signatures may use asymmetric encryption methods like Rivest-Shamir-Adleman (RSA). Secure key exchange enables sensor nodes to exchange keys and digitally sign messages to ensure validity safely. Problems may arise in resource-constrained WSNs-IoT environments due to the computational complexity of RSA operations, especially key creation and encryption/decryption.

Selection of CHS

The suggested ISFO algorithm selects CHs by using a distinct fitness function that is according to a variety of factors, which is shown below:

Average Distances Between CHs AND Sensor Nodes (SN)

It indicates the total distance between each $\mathrm{CH_j}$ (CH_j) and all $\mathrm{SN_s}$ (s_i). Utilize Equation (1) to determine their average.

$$\frac{1}{m}\sum_{i=1}^{N} distance\left(s_{i,}CH_j\right) \tag{1}$$

where *N* represents SN counts, and *m* represents counts of CHs.

Each node uses some energy when transmitting data to its CH. To limit the energy used, choose CHs near all the remaining SNs.

Average Distance Between CHS and BS

Equation (2) depicts ratios of CHs (*m*) to distances between each CH_j (CH_j) and each BS (*BS*).

$$\frac{1}{m} distance\left(CH_j, BS\right) \tag{2}$$

CHs start sending information acquired from SNs to the BS and hence need to be nearer to the BS. The lengths of time that separate CHs from BS and CHs from nodes can be obtained by combining Equation (1) and Equation (2) into Equation (3) (named it $f_{distance}$)

$$Min\ f_{distance} = \sum_{j=1}^{m}\frac{1}{m}\left(\sum_{i=1}^{N} distance\left(s_i, CH_j\right) + distance\left(CH_j, BS\right)\right) \tag{3}$$

Energy in total for CHs. The referenced parameter is the total amount of present energy for all the selected CHs. Select the best CHs to increase the amount. In other words, it seeks to minimize the (named it f_{energy}) term in Equation (4), which is the inverse of this sum. Nodes need energy to transmit data and hence nodes with higher energy than others are selected as CHs [28, 29]

$$Min\ f_{energy} = \frac{1}{\sum_{j=1}^{m}\left(E_{CH_j}\right)} \tag{4}$$

E_{CH_j} signifies CH j's energy where $(1 \le j \le m)$.

The fitness function can be created from the previous two functions, $f_{distance}$ and f_{energy} by combining them into singular functions i. e. $f_{fitness}$ and depicted as Equation (5).

$$\begin{aligned}
&Min\ F_{fitness} = \alpha \times f_{distance} + (1-\alpha) \times f_{energy} \\
&s.t. \\
&distances\left(s_i, CH_j\right) \le R\ \forall_{s_i} \epsilon SN_s, CH_j \epsilon C \\
&distance\ \left(CH_j, BS\right) \le R_{max}\ \forall CH_j \in\ C \\
&E_{CH_j} > TH_E\ ,\quad 1 \le j \le m \\
&0 <\propto< 1 \\
&0 < f_{distance}, f_{energy} < 1
\end{aligned} \tag{5}$$

Where All sensor nodes are grouped as SNs, while all CHs are grouped as C,$C = \{CH1, CH2, \ldots, CHm\}$, implies "threshold energy" required to be a CH, control parameter, *R* is SNs i 's max. communication range, and CH's max. communication range is $Rmax$. while minimizing values of fitness functions in Equation 5 in choosing best CHs, the optimal CHs have lower fitness values.

Formation of Clusters

Once the initial action is completed, the clusters begin to develop. "' WeightF ", a weighting function, is used to generate clusters, and it is dependent on the following variables:

CHs' balance energy to communicate with other SNs in their communication ranges, an SN si must connect to CH j (*CHj*) that has greater residual energy than other CHs. This is depicted in Equation (6): [30]

$$WeightF\ \left(s_i, CH_j\right) \propto E_{residual}\left(CH_j\right) \tag{6}$$

$E_{residual}\left(CH_j\right)$ is directing to the residual energy for a CH_j**.**

Distances Between CHs AND SN

It ought to connect to the nearest $\mathrm{CH_j}\ \left(CH_j\right)$ within its communication range for a sensor node s_i. This will enable people to use less energy. Thus

$$WeightF(s_i,) \propto \frac{1}{distance\,(s_i,CH_j)} \tag{7}$$

Distance Between CHs and BS

The CHs are responsible for collecting data through SNs and sending it to the BS. SN s_i should join CHs closer to the BS since other CHs are farther away in their communication range.

$$WeightF(s_i, CH_j) \propto \frac{1}{distance\,(CH_j,BS)}. \tag{8}$$

Degree of the CH Node

A SN s_i must combine with a CHj (CHj) that has the fewest node degrees within its communication range. Given

$$weightF(s_i, CH_j) \propto \frac{1}{node\_degree\,(CH_j)} \tag{9}$$

Combine the prior Equations (7), (8), and (9) in Equation (10).

$$weightF(s_i, CH_j) \propto \frac{E_{residual}(CH_j)}{distance(s_i,CH_j)} \times \frac{1}{distance(CH_j,BS)} \times \frac{1}{node\_degree\,(CH_j)} \tag{10}$$

Thus, final functions of weights in cluster formations are based on Equation (11) [31]

$$weightF(s_i, CH_j) = C \times \frac{E_{residual}(CH_j)}{distance\,(s_i,CH_j)} \times \frac{1}{distance(CH_j,BS)} \times \frac{1}{node\_degree(CH_j)} \tag{11}$$

A constant named C is used with value = 1. SNs need to compute their $WeightF$ according to Equation (11) to form clusters, and join CHs with largest weights.

4. PROPOSED METHODOLOGY

An improved algorithm for Selection of CHs and Secure Data Communication in WSNs is presented in this work. It attempted to address the drawbacks of earlier research on secure data communication in wireless sensor networks by several authors [18, 32]. The suggested technique aims to provide high security while using the most restricted resources in WSN.

4.1. Sunflower Optimization Algorithm (SFO)

The Sunflower optimization algorithm (SFO), which was motivated by nature, has been introduced. The program mimics how two sunflowers that are close to one another spread pollen as they move toward the sun [19]. The following sections illustrate the traits and primary operations of the SFO algorithm (Figure 1).

The Natural Behaviors

When the sunflowers face the sun in the morning, the two nearest ones, X_i and $X_i + 1$, can be pollinated. Each sunflower takes in the sun's rays. The total radiation output of each sunflower is affected by its distance from the sun. Sun radiation (heat) from

sunflowers decreases as distance from the sun increases. Equation (12) demonstrates the amount of heat the sun receives.

$$Q_i = \frac{W}{4\pi c^2} \tag{12}$$

Where Q_i implies received heat values, W represents sun's energy, and c signifies distances between optimal solutions(sun) X^* and sunflowers X_i.

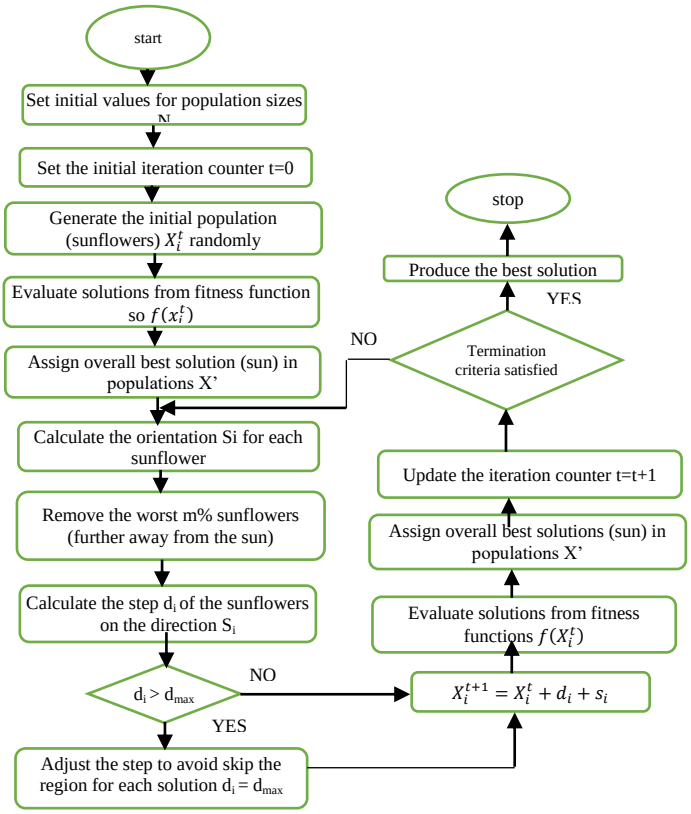

Figure 1: Displays the SFO algorithm's primary operations

The Sunflower Orientation Adjustment Process

Each sunflower's orientation vector is determined according to Equation (13)

$$\underset{s_i}{\rightarrow} = \frac{X^* - X_i}{\|X^* - X_i\|} \qquad i = 1,2,\ldots,N. \tag{13}$$

here X^* is the global optimal solution, X_i is solution i, and N is the population size.

Step Size of the Sunflowers Toward the Sun

According to Equation (14), the step size of each sunflower X_i toward the sun is determined.

$$d_i = \propto \times P_i(\|x_i + X_{i-1}\| \times \|X_i + X_{i-1}\|) \quad (14)$$

Where α represents sunflower's inertial displacements, $P_i = (\|X_i - X_{i-1}\|)$ represents pollination probabilities amongst sunflowers X_i and X_{i-1}. Sunflowers closest to the sun move more slowly to adjust their locations, while sunflowers further distant sway randomly. To stop each solution's border from being skipped, the max. step sizes for all sunflowers is limited to d_{max}. According to Equation (15), each sunflower'smaximum step size is determined.

$$d_{max} = \frac{\|X_{max} - X_{min}\|}{2 \times N} \quad (15)$$

where X_{max} is the upper bound, X_{min} is the lower bound, and N is the population size.

Fertilization Process

Sunflowers reproduce best by fertilizing areas around the sun where sunflowers' fertilization procedures can be signified by Equation (16),

$$X_{i+1} = X_i + d_i \times \underset{s}{\rightarrow}_i \quad (16)$$

Where X_{i+1} is a newly generated sunflower.

4.2. An Improved Sunflower Optimization Algorithm (ISFO) For Selection of CHs

The standard SFO method is prone to local minima trapping and has a slow convergence rate. The Improved Sunflower Optimization algorithm (ISFO) was created by applying the lèvy flight operator to the Typical Sunflower Optimization algorithm (SFO) to boost the diversity search. The SFO may prevent converging rapidly by getting caught in the local minima using the lèvy flight operator approach. The ISFO technique uses the same fundamental steps as the standard SFO technique, with the difference that Equation 14's step size is replaced by the lèvy flight operator, as shown in Equation 17.

$$X_{i+1} = X_i + levy(v) \times \underset{S_i}{\rightarrow} \quad (17)$$

Here, Levy (ν) is the lèvy distribution.
Algorithm 1 presents the suggested ISFO algorithm's framework.

Algorithm 1: The ISFO Algorithm

1: Set metric values for mortality rates m, population sizes N, rates of pollination P and max. iterations maxitr.

2: Set counter of iterations t: =0.

3: Primary populations $X_i^{(t)}$ are arbitrarily created, i=1…., N.

4: Estimate the fitness function for all solutions (sunflowers) in the population $f(X_i^{(t)})$.

5: Finest solutions are assigned X*

6: repeat.

7: Utilizing Equation 13, solutions change their directions toward the sun (ideal solutions) x*.

8: To substitute the poorest m% solutions, new individuals are added to the population.

9: Using the levy flight operator from Equation 17, the solutions revise their positions.

```
10:  Estimate fitness functions for novel solutions (sunflowers) in
populations f(X_i^(t)).
11: If the new solutions are more fit than the ones already in place,
they will be adopted.
12:  Set t=t+1.
13: Until (t> maxitr)
14: The optimal resolution is provided.
```

It summarizes the stages of the suggested ISFO algorithm 1 as follows.

- **Parameter initialization:** Initialization of the parameters: The maximum number of iterations (maxitr), the population size (N), the mortality rate (m), and the rate of pollination (P) are the beginning values of the parameters.
- **Initialization of the iteration counter:** There is zero in the initialization counter.creation of solutions.
- **Solutions generation:** The population's solutions are generated randomly $X_i^{(t)}$
- **Assessment of the solutions:** The Fitness function for each population-level solution is $f\left(X_i^{(t)}\right)$
- **global best solution:** The greatest solution available worldwide.the best overall solution that was selected.Modification of solutions.
- **Solutions adjustment:** Equation 13 illustrates how the solutions approach the sun (ideal solution).
- **worst solution is mortality:** Mortality is the worst possible solution. The solutions with the lowest percentage of the population are removed, and new ones are presented. Updates on solutions.
- **Solutions update:** Equation 17 illustrates how the Lévy flight operator is used to update the solutions in order to avoid premature convergence and getting caught on the local minima.
- **new solutions evaluations:** The assessment of the new solutions.In the fitness function of the population, each novel solution is denoted by $f\left(X_i^{(t)}\right)$.the most recent worldwide greatest option.
- **new global best solution:** The updated best option is selected.
- **Increase the iteration counter:** The iteration counter $t = t + 1$ is increasing.fulfillment of the termination requirements.
- **Termination criteria:** The processes carry on until max. iterations maxitr is accomplished.
- **The global best solution:**The optimal resolution is provided.

4.3. Cryptography Techniques for Secure Data Transmission

Cryptographic techniques are primarily utilized as a crucial component of the WSN's security architecture to prevent the attacks mentioned above and accomplish data security in WSNs. Cryptography techniques compress basic data packets into secured data packets containing coded data instead of transmitting original data packets directly in networks [20]. Encrypted data, which functions as a layered network model, is often made up of an additional set of bits added to the original data that are safe and consistent with the existing protocols throughout the network, preventing attackers from accessing the original data during transmission. Two cryptography techniques can satisfy the

essential security requirements of secrecy and integrity in networks. Asymmetrical and Symmetric Cryptography (public and secret keys)

4.3.1. Symmetrical Cryptography / Symmetric Encryption/Secret Key Cryptography

Chosen earlier and use a single secret key kept hidden in a network, as indicated in Figure 2, for both decryption and encryption of data packets in a communicative network. Block and stream cyphers are two more categories for symmetric key algorithms used for fixed and time-varying transformations [21]. These two subcategories are used to examine encryption methods at different degrees on plain texts while taking different data kinds, battery consumption factors, data block sizes, and key sizes into account.14, 15, and different speeds of encryption and decoding 7, 8.

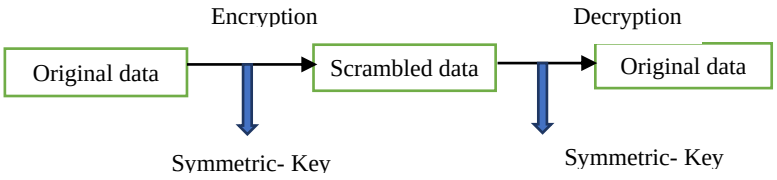

Figure 2: Symmetric – key cryptography

The most challenging duty in the network is keeping the key a secret. The WSN12-15 algorithms AES, DES, RC4 CAST, and RC5 are examples of symmetric key cryptosystems.

4.3.2 Asymmetric Cryptography / Asymmetric Encryption / Public Key Cryptography

Asymmetrical cryptography, utilized frequently, employs private and public keys for data decryption and avoids key sharing in a network, as shown in Figure 3.A public key and a private key are the building blocks of an asymmetric encryption technique, which is also called public-key encryption. A public key and a private key, or key pair, must be generated initially. One uses the receiver's public key to encrypt a message before sending it to the key pair's owner. If the receiver has the matching private key, they may use it to decipher the encrypted message. Digital signatures, which testify to the authenticity and legitimacy of a document or communication, are also created using asymmetric encryption techniques.

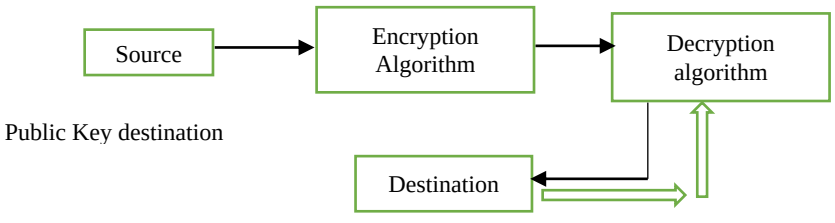

Figure 3: Asymmetrical key cryptography

By comparing their public and private keys with the sender's, people who have the corresponding private key can decrypt the data at the recipient end. Because the

encrypted data is never made publicly available to all users, but is only made available to those who are permitted to access it, the keys function as two-way security providers.

Asymmetrical Cryptography Implementations

Asymmetrical public key cryptography Since symmetrical methods of security avoidance are less effective than cryptographic ones, and cryptography is primarily employed as an implemented cryptography methodology. Public keys are related but distinct, as stated in their fundamental theory.

- publicly available;
- privately chosen by the user.

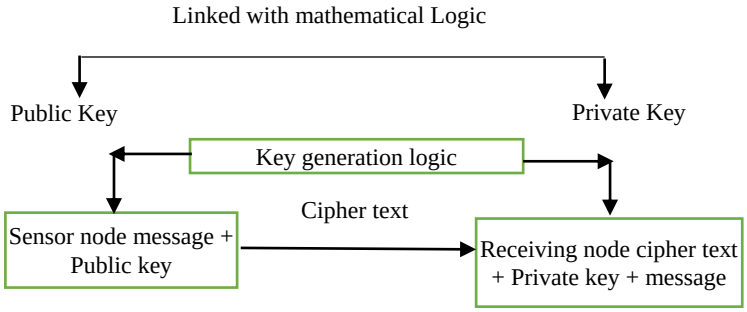

Figure 4: Public key cryptography

As shown in Figure 4, the keys are related but computationally distinct, making it impossible to ascertain private keys using public keys. As a result, higher-level attacks are prevented by utilizing these cryptography algorithms, which also reduce security complexity by avoiding networks with known keys. WSNs12 often support using asymmetric public key cryptosystems such as Diffie-Hellman key agreement14, 15, ECC, or RSA signatures.

5. RESULTS AND DISCUSSION

Using MATLAB R2019b and a Windows 10 Pro (64-bit) computer with an Intel Core i5 processor running at 2.30 GHz and 8 GB of RAM, the suggested ISFO method was developed. Throughput, energy usage, data transfer rate, and network lifetime are compared between the current and suggested techniques [22, 23].

Table 1: Experimental Setup

Parameters	values
Areas	1000m2
Nodes	100
Initial energies	0.1 J
Bandwidths	20kbps
sizes of packets	500 bytes
Distributions of nodes	random
total nodes	500

Throughput

When a packet is delivered, the throughput is determined by counting how many packets were received in that period. Equation (18) is used to calculate throughput.

$$Throughput = \frac{N_r}{T} \times 100\% \tag{18}$$

where Nr signifies the aggregate sum of the nodes, and T signifies the simulation time.

Packet delivery ratio

According to Eq. (19), the PDR is calculated by dividing the total number of packets delivered by the source node by the total number of packets received at the endpoint.

$$PDR = \frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\% \tag{19}$$

where X is signified as the number of packets received, Y is signified as the number of packets sent, i is signified as

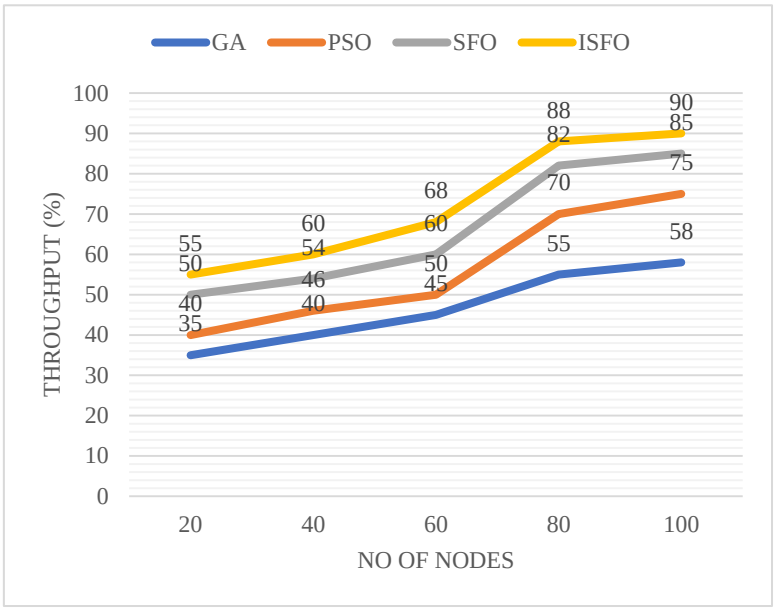

Figure 5: Throughput results

Figure 5 illustrates the comparison between the GA [24], PSO [25], and SFO techniques for throughput. Compared to the current GA, PSO, and SFO methods, the throughput of the ISFO approach is high in this instance [26, 27]. The suggested ISFO method's fitness functions increase the system's total throughput.

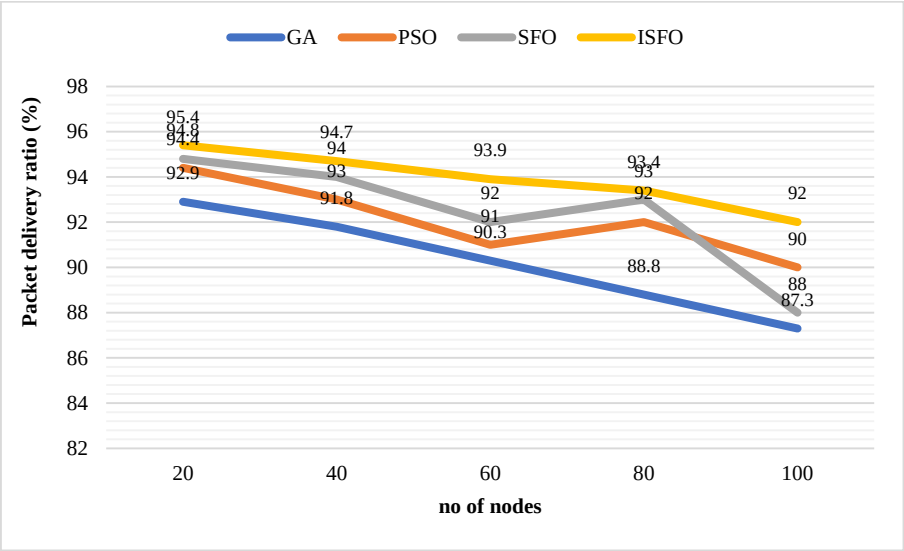

Figure 6: Packet delivery ratio results

Figure 6 illustrates the comparison between the GA, PSO, SFO and ISFO methodsaccording toPDR. The suggested ISFO approach outperforms the current GA, PSO, and SFO methods in performance. By computing the nodes' trust values and the communication cast using the fitness function computation, the suggested technique's PDR is ISFO.

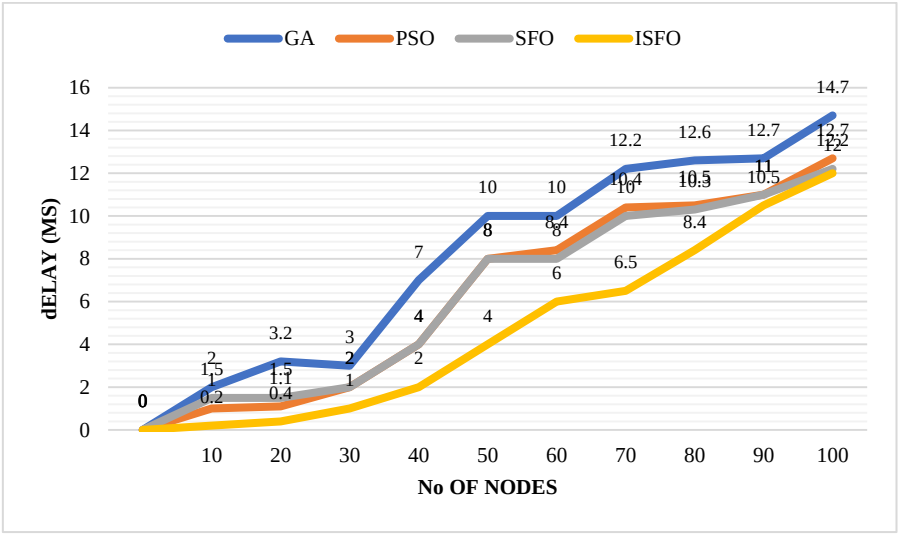

Figure 7: Delay results

Figure 7 illustrates the comparison between the GA, PSO, SFO and ISFO methodsaccording to delay. When comparing current GA, PSO, and SFO, the delay of the IBFA-EHC method is minimal. The fitness function considers communication cost and trust value to prevent link failure during data transmission. As a result, there is only minimal lag when transmitting data.

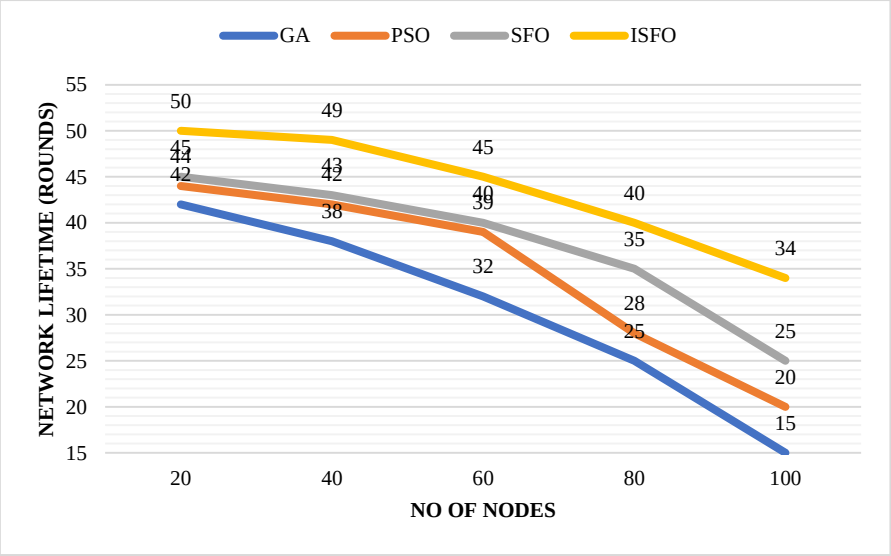

Figure 8: Network lifetime results

The network lifetime for the specified packet size is shown in Figure 8. The Number of nodes is measured on the x-axis, and the network lifetime is measured on the y-axis. The suggested ISFO technique considerably extends the lifetime of the sensor node during data packet transmission. Due to the use of the cryptography algorithm when performing CH-based data transmission, it has been found that the suggested method extends the network lifetime as packet sizes grow. It demonstrates that the suggested method offers a longer network lifetime than the other current GA, PSO, and SFO algorithms.

5. CONCLUSION

This study uses the suggested ISFO protocol to improve the choice of CH nodes and secure data transmission via WSN. Here, the ISFO algorithm is suggested to discover the optimal CH node selection. The best CH node is selected using fitness indicators. Fitness function, throughput, remaining energy, and end-to-end delay are all factors that must be considered when selecting a CH node to achieve the optimal outcome. Using route discovery and route maintenance functions to promote secured multipath routing data transfer, the cryptographic approaches protocol aims to boost WSN performance. Protocols using cryptography techniques bypass attack nodes, significantly reducing packet loss. The security technique algorithm safeguarded the data transfer, which boosts WSN performance. The outcome shows that compared to the existing methodologies, the

suggested ISFO-cryptography technique approach offers higher throughput of 90.2%, data transfer rate of 95.5%, network lifetime of 12.2%, and lower energy usage of 10.3%.The limitation of this study is that network lifetime is low compared to other existing methods. Future research may examine how well the suggested framework performs in an IoT network. Additionally, novel encryption algorithms and hybrid swarm optimization can be created to deal with computational complexity difficulties effectively.

Conflict of interest statement: No conflicts of interest have been revealed by the author.

Funding: This research received no external funding.

REFERENCE

[1] K.A. Darabkh, M.Z. El-Yabroudi and A.H. El-Mousa, "BPA-CRP: A balanced power-aware clustering and routing protocol for wireless sensor networks," *Ad Hoc Networks*, vol. 82, pp. 155-171, 2019.

[2] A. Onasanya, S. Lakkis and M. Elshakankiri, "Implementing IoT/WSN based smart Saskatchewan healthcare system," *Wireless Networks*, vol.25, no. 7, pp. 3999-4020, 2019.

[3] S. Sivakumar and P. Vivekanandan, "Efficient fault-tolerant routing in IoT wireless sensor networks based on path graph flow modeling with Marchenko–Pastur distribution (EFT-PMD)," *Wireless networks*, vol. 26, no. 6, pp. 4543-4555, 2020.

[4] C. Iwendi, P.K.R. Maddikunta, T.R. Gadekallu, K. Lakshmanna, A.K. Bashir and M.J. Piran, "A metaheuristic optimization approach for energy efficiency in the IoT networks," Software: Practice and Experience, vol. 51, no. 12, pp. 2558-2571, 2021.

[5] K. Gangadharan, G.R.N. Kumari, D. Dhanasekaran and K. Malathi, "Detection and classification of various pest attacks and infection on plants using RBPN with GA based PSO algorithm," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 20, no. 3, pp. 1278-1288, 2020.

[6] T. Wang, X.Qin, Y. Ding, L. Liu and Y.Luo, "Privacy-preserving and energy-efficient continuous data aggregation algorithm in wireless sensor networks," *Wireless Personal Communications*, vol. 98, pp. 665-684, 2018.

[7] K. Gangadharan, G.R.N. Kumari, D. Dhanasekaran and K. Malathi, "Automatic detection of plant disease and insect attack using effta algorithm," *International Journal of Advanced Computer Science and Applications*, vol.11, no. 2, 2020.

[8] S.R. Nabavi, V. Ostovari Moghadam, M. Yahyaei Feriz Hendi and A. Ghasemi, "Optimal selection of the cluster head in wireless sensor networks by combining the multiobjective genetic algorithm and the gravitational search algorithm," *Journal of Sensors*, pp. 1-16, 2021.

[9] Y. Lin, N. Tong, M. Shi, K.Fan, D. Yuan, L. Qu and Q. Fu, "K-means optimization clustering algorithm based on particle swarm optimization and multiclass merging," In Advances in Computer Science and Information Engineering, Springer Berlin Heidelberg, Vol. 1, pp. 569-578, 2012.

[10] S. Yang, B. Zhao and Y. Peng, "Cluster head selection algorithm based on levy flight butterfly optimization algorithm in WSN," In International Conference on Cloud Computing, Performance Computing, and Deep Learning (CCPCDL 2022), Vol. 12287, pp. 144-148, 2022.

[11] N.B. Patil, "Secure and Efficient Data Transmission for Cluster Based Wireless Sensor Network Using Cryptography", *International Journal of Advanced Engineering Research and Science*, vol. 4, no. 3, pp. 196-204, 2017.

[12] D. Sivakumar, S.S. Devi and T. Nalini, "Energy aware clustering protocol using chaotic gorilla troops optimization algorithm for Wireless Sensor Networks," *Multimedia Tools and Applications*, vol. 83, no. 8, pp. 23853-23871, 2024.

[13] S. Shitharth, H. Manoharan, A. Shankar, R.A. Alsowail, S. Pandiaraj, S.A. Edalatpanah, and W. Viriyasitavat", Federated learning optimization: A computational blockchain process with offloading analysis to enhance security", *Egyptian Informatics Journal*, vol. 24, no. 4,, p.100406, 2023.

[14] V. Verma and V.K. Jha, "Secure and energy-aware data transmission for IoT-WSNs with the help of cluster-based secure optimal routing," *Wireless Personal Communications*, vol. 134, no. 3, pp. 1665-1686, 2024.

[15] S.E. Najafi, H. Nozari and S.A. Edalatpanah, "Investigating the Key Parameters Affecting Sustainable IoT-Based Marketing," In Computational Intelligence Methodologies Applied to Sustainable Development Goals, Cham: Springer International Publishing.pp. 51-61, 2022.

[16] M.S. Deelip and G. Kannayaram, "Exponential-sunflower optimization and deep convolution neural network for secure routing and prediction in internet of things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 4, pp. 4201-4220, 2023.

[17] A.F. Raslan, A.F. Ali, A. Darwish and H.M. El-Sherbiny, "An improved sunflower optimization algorithm for cluster head selection in the internet of things," IEEE Access, vol. 9, pp. 156171-156186, 2021.

[18] A. Chinnappa and C. Vijayakumaran, "An Effective Signcryption with Optimization Algorithm for IoT-enabled Secure Data Transmission," Computers, Materials & Continua, vol. 73, no. 2,2022.

[19] Z. Yuan, W. Wang, H. Wang and N. Razmjooy, "A new technique for optimal estimation of the circuit-based PEMFCs using developed sunflower optimization algorithm," *Energy Reports*, vol. 6, pp. 662-671, 2020.

[20] H. Dogra and J. Kohli, "Secure data transmission using cryptography techniques in wireless sensor networks: a survey," *Indian Journal of Science and Technology*, 2016.

[21] P.P. Santoso, E. Rilvani, A.B. Trisnawan, K. Adiyarta, D. Napitupulu, T. Sutabri and R. Rahim, "Systematic literature review: Comparison study of symmetric key and asymmetric key algorithm," In IOP Conference Series: Materials Science and Engineering, Vol. 420, pp. 1-6, 2018.

[22] B.M. Sahoo, H.M. Pandey and T. Amgoth, "A genetic algorithm inspired optimized cluster head selection method in wireless sensor networks," *Swarm and Evolutionary Computation*, vol. 75, pp. 101151, 2022.

[23] B. Singh and D.K. Lobiyal, "Energy-aware cluster head selection using particle swarm optimization and analysis of packet retransmissions in WSN," *Procedia Technology*, vol. 4, pp. 171-176, 2012.

[24] A. Rahiminasab, P. Tirandazi, M.J. Ebadi, A. Ahmadian and M. Salimi, "An energy-aware method for selecting cluster heads in wireless sensor networks," *Applied Sciences*, vol. 10, no. 21, pp. 7886, 2020.

[25] S. VenkataRao and V. Ananth, "A Hybrid Optimization Algorithm and Shamir Secret Sharing Based Secure Data Transmission for IoT based WSN," *International Journal of Intelligent Engineering & Systems*, vol. 14, no. 6, pp. 498-506, 2021.

[26] D. Paulraj, R. Lavanya, T. Jayasudha, M.I. Niranjana, T. Daniya and F.D. Shadrach, "Blockchain-based Wireless Sensor Network Security Through Authentication and Cluster Head Selection," In 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS),pp. 1-5, 2023.

[27] N. Vidhya, V. Seethalakshmi, R. Monisha, J.Dhanasekar, V. Gurunathan and C. Rajanandhini,

"Coherent Data Transmission Using Multiplexing for a DWDM Communication System," In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), pp. 1-4, 2022.

[28] F. Taghvaei and R. Safa, "Efficient energy consumption in smart buildings using personalized NILM-based recommender system," *Big data and computing visions*, vol. 1, no. 3, pp. 161-169, 2021.

[29] K. Bagherzadeh Asl and A. Alburaikan, "Survey on low energy adaptive clustering hierarchical protocol," *Big data and computing visions*, vol. 2, no. 3, pp. 112-116,2022.

[30] B.O. Saracoglu and M. De Simón Martín, "Initialization of a multi-objective evolutionary algorithms knowledge acquisition system for renewable energy power plants," *Journal of applied research on industrial engineering*, vol. 5, no. 3, pp. 185-204, 2018.

[31] G.F. Belay, "Energy wastage on an automobile due to speed breakers: a case study on Woldia town," *International Journal of Research in Industrial Engineering*, vol. 9, no. 2, pp. 202-208,2020.

[32] S.A. El-Morsy, "Comparison between domestic and hostile applications of wireless sensor networks," *Computational algorithms and numerical dimensions*, vol. 1, no. 1, pp. 30-34, 2022.