Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.020969
Article

Tech Science Press

Intelligent Chimp Metaheuristics Optimization with Data Encryption Protocol for WSN

P. Manjula[1,*] and Dr. S. Baghavathi Priya[2]

[1]Department of Information Technology, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, Tamil Nadu, 600062, India
[2]Department of Computer Science and Engineering, Rajalakshmi Engineering College, Thandalam, Tamil Nadu, 602105, India
*Corresponding Author: P. Manjula. Email: manjula.arunraj@gmail.com
Received: 17 June 2021; Accepted: 17 August 2021

Abstract: Recent developments in low power electronic devices integrated into wireless communication technologies resulted in the domain of wireless sensor networks (WSN), which finds in applications in diverse data gathering and tracking applications. Since WSN is mostly deployed in harsh and inaccessible environments, it is necessary to design energy efficient and security solutions. The clustering technique is an effective way to lengthen the lifetime of WSN. But most of the clustering techniques elect cluster heads (CHs) irrespective of clusters. To resolve this issue, this paper presents a new intelligent metaheuristics based energy aware clustering with data encryption protocol (IMEAC-DEP) for WSN. The goal of the IMEAC-DEP technique is to elect an appropriate set of CHs and CHs to encrypt the data prior to intercluster communication. The proposed IMEAC-DEP model involves two major phases namely clustering and data encryption. At the first stage, a new chimp optimization algorithm based clustering (COA-C) technique is derived with four fitness parameters. Next, in the second stage, signcryption with artificial fish swarm optimization algorithm (SC-AFSA) based data encryption technique is derived. In order to validate the performance of the proposed IMEAC-DEP model, a series of experiments were performed and the results are investigated under different aspects. The resultant experimental values highlighted the superior performance of the IMEAC-DEP model over the recent stage of art methods interms of energy efficiency as well as security.

Keywords: Energy efficiency; clustering; security; data encryption; metaheuristics; wireless sensor networks

1 Introduction

Wireless sensor network (WSN) contains several sensors dispersed in space that is utilized for monitoring and sense the environments like humidity, temperature, sound, light, pressure, vibration, military terrain, and location for transferring data to base station (BS) via network to process [1]. WSN is a stimulating study area for several researchers and acts as a significant part of cloud computing (CC),

edge computing, Internet of Things (IoT), etc. WSN might be placed in difficult remote platforms. The network is highly susceptible to few malicious attacks because of its unattended policy of placement. Furthermore, sensor nodes have constrained resources and battery power, hence energy efficiency is the most crucial problem confronted by all WSNs. The Energy Consumption (EC) on a wireless network could be reduced by separating the sensor node as cluster heads (CHs). CH is in charge to authenticate the nodes which are permitted to join a cluster and interact with a network. Consumption of more assets might cause negative effect on network lifetime. Thus, WSN should utilize the minimum power consumption for attaining highest security to attain secured transmission between nodes [2]. Henceforth, optimum energy consumption, thus maximizes the lifetime of network and ensuring security, is of major significance in an environment needing higher security. But, if numerous sensors transmit several data to a similar CH, it can be easier for the CH energy that exists exhausted when it doesn't offload the neighbour CHs [3]. The convenience of CH facilities in routing switching, data fusion, and other technologies was highly enhanced.

WSN security approaches are generally utilized for preventing attacks. Usually, the passive & active attacks are feasible in the WSN [4]. The active attacks are additionally categorized to control, privacy, and attacks to privacy. The main threat to privacy is eavesdropping [5]. It performs as a learner/listener for securing the data. This kind of attacker forges the data and responds to the queries with incorrect responses. This kind of attacker is named as Man in the middle attackers. Other significant attacks are byzantine, this kind of attackers can simply compromise the node and take overall controls on them and perform as legitimate clients [6]. Wormhole and Black holes are the few attacks belonging to this classification [7]. It can be stated that utilizing a single conventional symmetric key isn't safe; for the reason that sensor nodes aren't tamper proof and taken by attackers, whole information would be revealed to the attackers [8].

This paper presents a new intelligent metaheuristics based energy aware clustering with data encryption protocol (IMEAC-DEP) for WSN. The IMEAC-DEP technique intends to choose a proper set of CHs and CHs to encrypt the data prior to intercluster communication. The proposed IMEAC-DEP model involves a new chimp optimization algorithm based clustering (COA-C) technique for optimal selection of CHs and construction of clusters. The COA is chosen due to the fact that it alleviates the problems of slow convergence rate and trapping in local optima. Besides, a signcryption with artificial fish swarm optimization algorithm (SC-AFSA) based data encryption technique is employed for secure intercluster communication. The AFSA has good robustness, global search ability, tolerance of parameter setting, and it is also proved to be insensitive to initial values. The design of COA-C and SC-AFSA shows the novelty of the work. For examining the enhanced outcome of the proposed IMEAC-DEP model, an extensive set of simulations take place and the outcomes are examined interms of different measures. In short, the key contributions of the paper are listed as follows.

- Propose an IMEAC-DEP technique to achieve energy efficiency and security in WSN by the use of metaheuristic optimization algorithms
- Aims to elect an appropriate set of CHs and CHs encrypt the data prior to intercluster communication.
- Designs a new COA-C technique to select optimal CHs and construct clusters. To the best of our knowledge, none of the earlier works have derived a clustering technique using COA.
- Derive a new SC-AFSA based encryption technique, which includes an optimal key generation process of SC using AFSA in such a way that the security can be enhanced at the CHs.
- Validate the energy efficiency and security performance of the proposed IMEAC-DEP technique over the recent state of art methods.

The paper is structured as follows. Section 2 briefs the existing clustering and security based solutions in WSN. Besides, Section 3 describes the system model. Then, Section 4 elaborates the proposed IMEAC-DEP

technique and Section 5 validates the performance of the proposed model. Lastly, Section 6 concludes the paper.

2 Literature Survey

This section performs a comprehensive review of existing metaheuristic algorithm based clustering techniques and security based solutions available in the literature for WSN.

2.1 Existing Works on Energy Aware Clustering Techniques

Pan et al. [9] proposed a new optimization method, like compact bat algorithm (cBA), to utilized class of optimization problem including devices that contain restricted hardware assets. Research determines that the presented method to attain an efficient manner to utilize restricted storage device and gives reasonable outcomes. In Wang et al. [10], a certain clustering technique named Energy Centres Searching utilizing Particle Swarm Optimization (EC-PSO) is proposed for avoiding energy holes and search energy centres for selecting CH. The Energy centres are examined by an enhanced PSO method and nodes near the energy centre are selected as CH.

Ahmad et al. [11] propose a novel method for CH selection based on Artificial Bee Colony (ABC) optimization. The FF for ABC is estimated depending upon 3 variables namely intra cluster distance, RE, and distance from sink stations. They enhanced the FF by utilizing ABC optimization. The Opposition based Chaotic Whales Optimization algorithm (OBC-WOA) is Metaheuristic optimization method that has been currently presented in opposition [12]. It simulates humpback whale social behaviors. The OBCWOA generates arbitrarily its population in exploitation and exploration phases, as another population based system that could generate the value farther from optimum alternate/block improvement of local optimal. The studied method so called OBCWOA is implemented to raise the solution reliability and precision. The OBCWOA utilizes a method that is depending upon opposition to enhance the effectiveness of OBCWOA. The OBCWOA is separated with primary WOA method and another Meta heuristic method. The efficiency of presented method is calculated based on throughput, PDR, NLT, and EC. Chandirasekaran et al. [13] utilize novel evolution method, cat swarm optimization (CSO), which is implemented and designed in real-world for minimizing the intra cluster distance among the CM and CH and enhance the energy dispersal for WSN. They examined the efficiency of WSN protocol using sensor nodes placed in an area and gathered to clusters. The outcome is related to the well-known protocol LEACH-C and swarm based optimization method PSO.

Solaiman [14] proposed an early concept on giving a hybrid clustering method depending upon K-means clustering and PSO; called KPSO to attain effective energy management of WSN. This KPSO method is related to conventional clustering methods like K-means clustering and LEACH protocol independently. Zhou et al. [15] presented a novel technique to extend the network lifespan depending upon enhanced PSO method that is an optimization technique implemented for selecting targeted node. The presented protocol leads to an improved distributed sensor and well balanced clustering method to enhance the network lifespan. They relate the developed protocol with relative protocols by differing the amount of variables that is network area size, amount of nodes, and location of BS. Baranidharan et al. [16] contributed a novel clustering method, Distributed Unequal Clustering using Fuzzy logic (DUCF) that selects CH by fuzzy method. The DUCF creates an uneven cluster for balancing the EC between the CH. In Cheng et al. [17], initially, they presented a spatial correlation method between sensed data with Markov Random Field (MRF) module. Next, they proposed a new Representative node Selection Procedure (RSP), energy effective Node Scheduling Algorithm (NSA), and Data Amendment Procedure (DAP), correspondingly for these aforementioned problems.

2.2 Existing Security Based Solutions in WSN

In Athmani et al. [18], an efficient dynamic authentication and key Management system are projected to heterogeneous WSN. The key distribution technique is depending on preceding data for generating dynamic keys and doesn't need sharing phase and secure channel that enhances the energy efficiency, security and decreases memory utilization. Zhou et al. [19] efficiently integrates security verification and LB and proposed a lightweight LB and verification system (secure load and energy balancing) depending upon clustered WSN. In Cui et al. [20], a blockchain based multi WSN authentication system for IoT is presented. A blockchain network is created amongst distinct kinds of nodes for creating hybrid blockchain modules like public chain and local chain. In Goyal et al. [21], secure authentication and protected data aggregation technique for the CH architecture of UWSN is presented due to cluster based arrangement generates a stable and concise networks. Similarly, the data being transmitted in the network would be safely managed for ensuring that it won't be compromised in the network processes. Guo et al. [22] proposed a power IOT information defence approach depending upon enhanced IIDC. Initially, the terminal devices set the private key for resolving the key problems of terminal security authentication in the IOT module. Simultaneously, the enhanced method actively creates pseudo cryptographic matrix for avoiding collusion attacks. Sureshkumar et al. [23] proposed an FSAC method that observes the distinct types of the data packet transferred with the sensor for avoiding attacks. The FSAC is executed for utilizing the effective routing path to reduce energy utilization. This technique detects the nearby transferring nodes to enhance the effective path system for the data packet routing by the FL technique. Kavitha [24] proposes a cryptographic based clustering structure to preserve data privacy by OPMDCRP which enhances data privacy and energy efficient routing for the heterogeneous network. This scheme gives higher data privacy using ECIES-KPM alongside smaller key sizes. Since WSN is mostly deployed in harsh and inaccessible environments, it is necessary to design energy efficient and security solutions. The clustering technique is an effective way to lengthen the lifetime of WSN. But most of the clustering techniques elect cluster heads (CHs) irrespective of clusters. Therefore, the security and energy efficient performance can be further improved by the use of proposed model.

3 System Model

Assume a network with N sensors in a targeted region with the transmission range R. The N sensor nodes are denoted as: $\{N_1, N_2, \ldots, N_n\}$. A sink is located in the sensing region it could stay static in the placed area [25]. Few expectations are created in the following sections.

3.1 Network Model

During node placement, the few assumptions that are interrelated to sensors are given as follows.

- Sensors or BS are static and arbitrarily placed in the network
- Whole sensors are homogenous
- All the sensor nodes are distributed to a unique ID in the IoT system
- The communication power of sensor nodes could be altered based on the transmission distance.

3.2 Energy Model

As batteries in the IoT based WSN are in-built and couldn't be easily replaced or recharged, the presented energy should be efficiently used for extending the network lifetime. The sensor consumes energy for distinct procedures like reception, processing, sensing, and transmission of data. A recent study stated that large amount of sensor energy is utilized to transmit data. In this research, first order radio energy model is utilized. The number of energy E_{tx} required for transmitting k bit data on the

distance d is given in Eq. (1).

$$E_{tx} = E_{elec}(k) + E_{amp}(k,d), \; = \begin{matrix} kE_{elec} + kE_{fs}d^2, \; d < d_0 \\ kE_{elec} + kE_{mp}d^4, \; d \geq d_0 \end{matrix} \tag{1}$$

whereas *Elec* denotes radio electron energy, and E_{mp} indicates transmitter amplification energy that comprises free space propagation energy E_{fs} and multipath propagation energy E_{mp} depending upon distance d_0, that is determined by Eq. (2):

$$d_0 = \sqrt{\frac{E_{fs}}{E_{mp}}} \tag{2}$$

If the communication distance doesn't go beyond d_0, E_{fs} is used and when it goes beyond d_0, E_{mp} is utilized. Further, the energy consumed to obtain k bits of data is determined by Eq. (3).

$$E_{rx} \; = \; E_{elec} \times \; k \tag{3}$$

4 The Proposed IMEAC-DEP Technique

The overall system architecture of the proposed IMEAC-DEP technique is illustrated in Fig. 1. The figure demonstrated that the sensor nodes in WSN are randomly deployed and are initialized together in the network. Then, the COA-C technique gets executed to select CHs. Once the CHs are elected, the nearby nodes join the CH and become CMs; thereby clusters can be constructed. Afterward, the SC-AFSA technique is utilized by the CHs to encrypt the data and the encrypted data is transmitted via CHs to BS. The detailed working of these processes is discussed in the succeeding sections.

4.1 Design of COA-C Technique

A new hunting based optimization technique named COA is stimulated using sexual motivation and individual intelligence of chimps in their group hunting unlike other social predators. In chimp colony, it has 4 kinds of chimp allowed for the hunting procedure called attackers, barrier, driver, and chaser [26]. They have distinct capabilities, however, these varieties are needed for an effective hunt. The part of every chimp in the hunting to attack the prey is classified under;

- **Driver:** It follows the prey without trying to catch up with it.
- **Barriers:** It is placed at the bottom of the trees and climbs to block prey that leaves in a distinct direction.
- **Chasers:** It moves quickly afterward the prey to catch up with it.
- **Attackers:** Lastly the attacker prognosticates the escaping route of the prey for inflicting the prey back to the chaser or down to the lowest canopy.

Male chimp hunts over and above females. If captured and killed, the meal is shared with entire hunting party members and bystanders. Chimpanzees are naturally closer to humans, and indeed, chimpanzees take part in around 98.6% of human's DNA. Humans take part further DNA with chimpanzees compared to monkeys or other groups. Since scientists structured the chimp genome, they have experienced that humans share around 99% of theirs DNA with chimpanzees, making them our closer living relations.

The procedure of location upgrading technique is the search chimp's position in the search space about the location of another chimp location. Later, the ultimate location is placed arbitrarily in a circle that is determined using driver, chaser, attacker, and barrier chimp locations. Specifically, the prey location is calculated using these 4 optimum groups and other chimps arbitrarily upgrade their locations with it.

The mathematical modeling of group attacking, blocking, driving, and chasing are determined as follows. For numerically chasing and driving the prey, it can be denoted as follows,

$$D = \left|C.\ A_{prey}(n) - m.\ A_{chimp}(n)\right| \tag{4}$$

$$A_{chimp}(n+1) = A_{prey}(t) - x.\ D \tag{5}$$

whereas n denotes amount of present iteration, c, m, and x indicates coefficient vector, which are the vector and prey positions of a chimp.

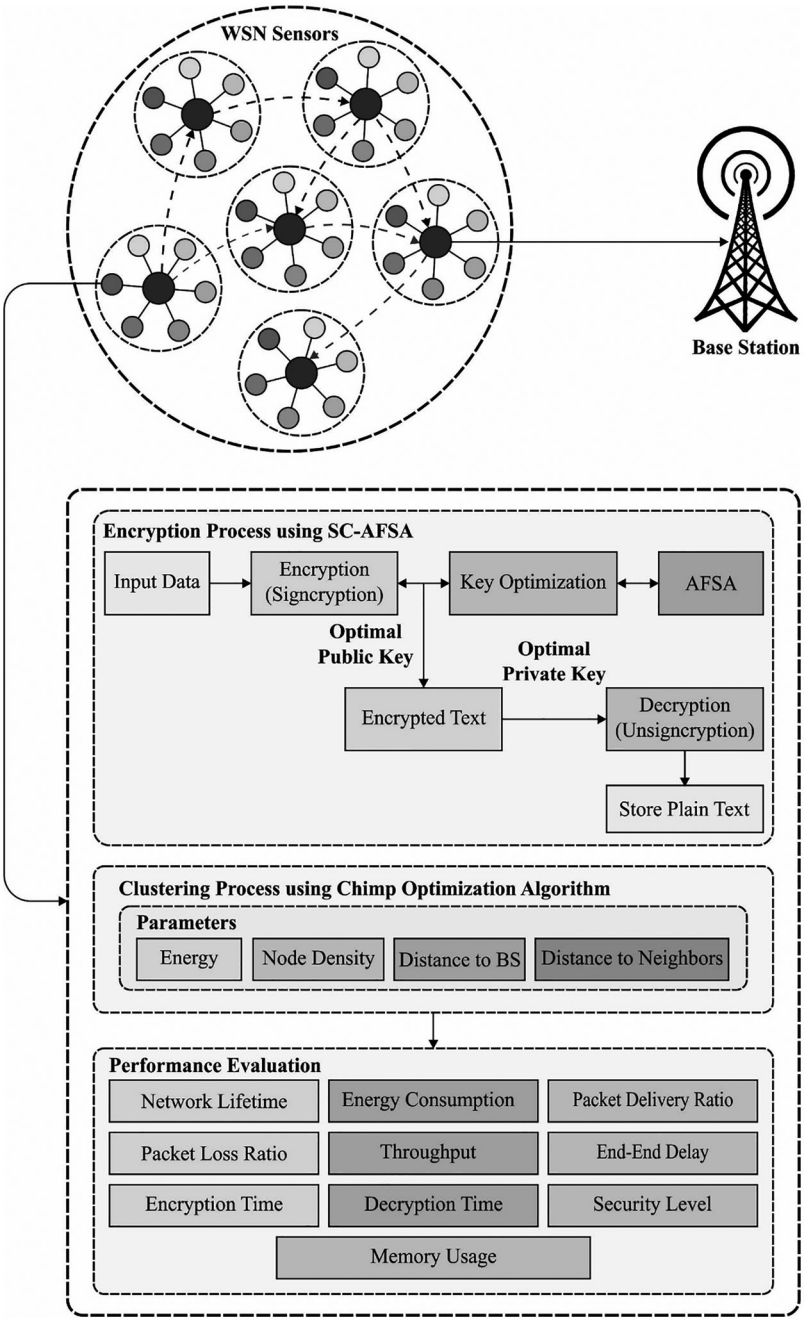

Figure 1: Workflow of IMEAC-DEP technique

The vectors c, m, x is estimated using,

$$X = 2.L.rand_1 - L \tag{6}$$

$$C = 2.rand_2 \tag{7}$$

$$M = chaotic\_value \tag{8}$$

whereas rand denotes arbitrary vector in the range of zero and one. Lastly, m denotes chaotic vector estimated according to several chaotic maps thus this vector denotes the impact on sexual motivation of chimps in the hunting procedure.

For numerically implementing the behaviour of chimps, it is considered that the initial optimum solutions are presented with chaser, barrier, driver, and attacker are informed better regarding the position of significant prey. Thus, the 4 optimum solutions are still attained is stored and other chimps are compelled for upgrading the position based on optimal chimp positions. These connections are given by,

$$D_{Attacker} = |C_1 A_{Attacker} - m_1 A| \tag{9}$$

$$D_{Barrier} = |C_2 A_{Barrier} - m_2 A| \tag{10}$$

$$D_{Chaser} = |C_3 A_{Chaser} - m_3 A| \tag{11}$$

$$D_{Driver} = |C_4 A_{Driver} - m_4 A| \tag{12}$$

If the arbitrary values in the range of [−1, 1], the following location of a chimp could be in another position among its present location and the location of the prey.

$$A_1 = A_{Attacker} - x_1(D_{Attacker}) \tag{13}$$

$$A_2 = A_{Barrier} - x_2(D_{Barrier}) \tag{14}$$

$$A_3 = A_{Chaser} - x_3(D_{Chaser}) \tag{15}$$

$$A_4 = A_{Driver} - x_4(D_{Driver}) \tag{16}$$

The whole formula is given by,

$$x_{(n+1)} = \frac{x_1 + x_2 + x_3 + x_4}{4} \tag{17}$$

The usual upgrading location technique/chaotic module for upgrading the location of chimps in optimization. The arithmetical module is given as follows:

$$A_{chimp}(n+1) = \begin{cases} A_{prey}(n) - x.D, & if\ \phi < 0.5 \\ chaotic_{value}, & if\ \phi > 0.5 \end{cases} \tag{18}$$

The COA-C technique derives a fitness function using four fitness variables such as energy efficiency, node density, distance to neighbors, and distance to BS. The fitness variables are defined as follows.

Energy: The CH performs various events like gathering, sensing, data transmission, aggregation, etc. A fitness variable to an efficient consumption of the network energy is given by Eqs. (19) and (20).

$$R_e = e(n_i),\ Avg_e = \frac{1}{n}\sum_{i=0}^{n} e(n_i) \tag{19}$$

$$f_1 = CH_{opt} * \frac{R_e}{Avg_e} = \frac{CH_{opt} * e(n_i)}{\frac{1}{n}\Sigma_{i=0}^{n} e(n_i)} \forall CH_{opt} = 5\%\ of\ n,\ e(n_i) = 0.5J\ or\ 1.\ 25J\ or\ 1.\ 75J \tag{20}$$

where, R_e, Avg_e, and n_i denotes node remaining energy, a network average energy, and overall amount of sensor nodes from network. CH_{opt} indicates optimal percentage of CH. An objective function f_1 demonstrates the ratio of entire network average energy and nodes remaining energy.

Node density: In intra cluster transmission, cost is a significant variable to increase the energy efficiency of the network. Otherwise, the network energy consumption is high whereas the cost function of cluster is defined by:

$$f_2 = \max\left(n(CH_1), n(CH_2), n(CH_3) n\left(CH_j\right)\right) \forall n = 2\ To\ 95,\ j = 1\ to\ 15 \tag{21}$$

where $n\left(CH_j\right)$ indicates amount of sensors in the range of j^{th} CH $\left(CH_j\right)$. The value of objective function f_2 should be maximum for selecting CH and utilizes in decreasing the energy depletion.

Distance to neighbors: In intra cluster transmission, sensor transmits the data to CH. If CH is distant from CM, later sensor reduces the energy if CH is closer to the member sensor nodes later it uses minimal energy.

$$f_3 = \frac{1}{n_{s\tau}} \sum_{i=0}^{n_{sr}} disT(CH,\ i)\ \forall dist(CH,\ i) = 1\ to\ 35\ m, n_{sr} = 1\ to\ 100 \tag{22}$$

whereas, n_{sr} and $dist(CH,\ i)$ denotes amount of sensors in sensing sequence and the Euclidean distance from nodes and CH in the sensing sequence of the corresponding cluster. Hence, the value of f_3 must be lesser when decreasing intra cluster transmission power.

Distance to BS: When executing CH selection, the distance between the CH and BS captures a significant function as while the selected CH is distant from the sink that uses energy rapidly is estimated as follows:

$$f_4 = \frac{1}{CH} \sum_{\mathrm{i=0}}^{\mathrm{CH}} dist(BS,\ CH_i)\ \forall dist(BS,\ CH_i) = 1\ to\ 70m,\ CH = 1\ to\ 15 \tag{23}$$

whereas, $dist(BS,\ CH_i)$ denotes Euclidean distance among BS and i^{th} (CH_i). Minimize the f_4 objective function declaration which selected CH isn't distant from BS. When the f_1, f_2, f_3, and f_4 function variables are calculated, the objective function is so called FF that is defined as follows:

$$F = Maximize\ Fitness\ = \alpha * f_1 + \beta * f_2 + \gamma * \frac{1}{f_3} + \delta * \frac{1}{f_4} \tag{24}$$

whereas, α, β, γ, and δ indicates weighted coefficients to f_1, f_2, f_3, and f_4 FF variables, respectively. A range of the weighted coefficients could vary between zero and one.

4.2 Design of SC-AFSA Based Encryption Technique

Once the CHs are chosen and clusters are constructed, the SC-AFSA technique is executed by the CHs to encrypt the data. The major aim of this study is to improve a data transmission protocol which offers authenticity, confidentiality, and integrity of the data. At first, the regular data is deliberated to the security procedure which is encryption/decryption modules, and AFSA based signcryption method is presented. The objective of optimum key selection in SC-AFSA technique is selecting the optimum

public and private keys in receiver and sender sides. Next to the data encryption, it is kept in the CJ = H, later optimum private key is utilized to the data decryption procedure, now the optimum keys are obtained according to the objective function. A new method for public key cryptography is Signcryption that concurrently fulfills the element of digital signature and open key encryption with lowest cost. This property includes Non-repudiation signcryption are, Unforgeability, Confidentiality, and Integrity. This study contains unsigncryption, key generation, and signcryption, process. The message forwarding of previously encoded data is much secured with the presented AFSA signcryption with an optimum selection of keys.

4.2.1 Key Generation

The Signcryption denotes public key primitives that establish 2 major cryptographic devices that can ensure nonrepudiation, privacy, and honesty. It concurrently executes the task of encryption and digital signature. This initiation procedure initiates the prime number, hash function with keys [27]. For improving the data security, the projected method uses the ideal private keys with the help of optimization procedure.

Initiation:- L_P Large prime number, L_f Large prime factor, I Integer with order L_f modulo L_P, selected arbitrarily from $[1, \ldots L_P - 1]$, *Hash* One way hash function, where output has at least 128 bits, L_P Keyed one way hash function, D Value selected arbitrarily $\left[1, \ldots L_f - 1\right]$.

Sender Key pair $((M_{k1}, N_{k1}))$

$$M_{k1} = Q^{A_{k1}} \bmod L_P \tag{25}$$

Receiver key pairs (M_{k2}, N_{k2})

$$N_{k2} = Q^{A_{k2}} \bmod L_P \tag{26}$$

4.2.2 Optimal Key Selection Using AFSA

To select the optimal keys for signcryption technique with an objective function of attaining maximum security level, AFSA technique is employed. AFSA is familiar SI optimization module based on the behavior of fish swarming. This technique is very useful for developing modules in exclusive intelligence to identify global optimum solutions and doesn't obtain gradient detail of the objective function. Now, an artificial fish explores food is based on foraging hierarchy of swarming nature and arbitrary behavior. Additionally, artificial fish allows mutual data communication until attaining a global optimal. The basic idea of AFSA is determined in the subsequent: an n-dimension space, assumes a fish swarm with N artificial fish. Assume $X = (x_1, x_2, \ldots x_n)$ implies the Position of artificial fish, and $Y = f(X)$ represents fitness at location X. Consider $d_{ij} = \|X_i - X_j\|$ is a distance between the location X_i and X_j, and *Visual* and *Step* indicate perceptive range and moving stage of artificial fish, correspondingly [28].

Foraging behavior

Assume X_i denotes present state of artificial fish, and select the state *Xj* randomly from *Visual* range. If $Yj < Yi$, then artificial fish is moved a *Step* in direction of $\left(X_j - X_i\right)$. Also, decided a state *Xj* in arbitrary fashion for selecting either it encounters forward condition. If the criteria aren't fulfilled, then arbitrary behavior is executed. The foraging nature employs the provided rule:

$$\tilde{X}_i = \begin{cases} X_i + Step \cdot \dfrac{X_j - X_j}{d_{ij}} \cdot rand, & if\ \left(Y_j < X_i\right) \\ random\ behavior, & otherwise \end{cases} \tag{27}$$

where $\tilde{X}_i$ denotes forthcoming state of an artificial fish, *rand* represents uniformly created values from zero and one.

Swarming behavior

In fish swarm, artificial fish X_i should seek intermediate position X_c of N_F artificial fish in current neighborhood $(d_{ij} <$ Visual$)$. If $(Y_C/N_F > \delta Y_i)$, the artificial fish X_i moves towards X_c. The mathematical function of swarming behavior is given by:

$$\tilde{X}_i = \begin{cases} X_i + Step \cdot \dfrac{X_c - X_i}{d_{i_C}} \cdot rand, & if \left(\dfrac{Y_c}{N_F} < \delta \cdot Y_i\right) \\ foragying\ behavior, & otherwise \end{cases} \tag{28}$$

where $\delta \in (0, 1)$ represents food concentration.

Following behavior

When X_{lbest} is a local optimal unit in current neighborhood of X_i. Then, $(Y_{lbest}/N_F > \delta Y_i)$, the artificial fish X_i move in a direction $(X_{lbest} - X_i)$. The mathematical equation of this behavior is given by:

$$\tilde{X}_i = \begin{cases} X_i + Step \cdot \dfrac{X_{lbest} - X_i}{d_{i,lbest}} \cdot r\c{m}d, & if \left(\dfrac{Y_{lbest}}{N_F} < \delta \cdot Y_i\right) \\ foraging\ behavior, & otherwise \end{cases} \tag{29}$$

Random behavior

The artificial fish decide a position arbitrarily from *Visual* range and travel to the corresponding location. It is so called default behavior.

Behavior selection

For AF, the predetermined behavior is executed and related, respectively. Thus, an optimum nature was determined to upgrade current state of AF.

Bulletin

It is employed to record an optimum state X_{best} in fish swarm. All AFs are related to equivalent states. If the criteria turn normal, then a bulletin may be updated.

Thus, AFSA employs a social nature of fish swarm for resolving the optimization problems, and it is very useful for fish self-information and environmental data to change the search direction for gaining optimum convergence and diversity. Henceforth, AF attains a location whereas the food resource is maximal. Although AFSA is highest in global optimization module for optimization problems, it is yet danger in converging sub optimum like metaheuristics. It is so called premature convergence of difficult optimization problems that result in decreased performance.

5 Performance Validation

The proposed model is validated in MATLAB R2014 tool. A detailed results analysis of the proposed model with existing techniques takes place interms of different measures. A network of 1000 nodes are deployed with a BS at the center of the sensing region. Tab. 1 offers a detailed security analysis of the

SC-AFSA with other techniques interms of different measures [29]. The resultant values showcased that the SC-AFSA technique has outperformed the other methods with maximum security level and minimum encryption time, decryption time, and memory usage. A detailed comparison study is made with the krill herd optimization based clustering (KHO-C), grey wolf optimization based clustering (GWO-C) and grasshopper optimization algorithm based clustering (GOA-C) techniques.

Table 1: Security analysis of SC-AFSA with other techniques

Measures	SC-AFSA	LWC-RFF	SC-PSO	SC
Security level (%)	97.54	96.21	93.98	90.34
Encryption time (s)	6.43	9.97	14.32	17.48
Decryption time (s)	4.56	6.78	9.01	11.23
Memory usage (Bytes)	108	176	192	203

The security level refers the robust key distribution mechanism in the network. On examining the results interms of security level, it is evident that the SC-AFSA technique has obtained a higher security level of 97.54% whereas the LWC-RFF, SC-PSO, and SC techniques have depicted a lower security level of 96.21%, 93.98%, and 90.34% respectively. At the same time, on examining the performance interms of encryption time, the SC-AFSA technique has gained the least encryption time of 6.43 s whereas the LWC-RFF, SC-PSO, and SC techniques have required an increased encryption time of 9.97, 14.32, and 17.48 s respectively. Moreover, on investigating the performance with respect to decryption time, the SC-AFSA approach has attained the worse encryption time of 4.56 s whereas the LWC-RFF, SC-PSO, and SC methods have required an improved encryption time of 6.78, 9.01, and 11.23 s correspondingly. Furthermore, on examining the performance interms of memory usage, the SC-AFSA technique has gained the least encryption time of 108 bytes whereas the LWC-RFF, SC-PSO, and SC algorithms have required a higher encryption time of 176 bytes, 192 bytes, and 203 bytes correspondingly.

A detailed comparative result analysis of the IMEAC-DEP technique with other techniques take place in Tab. 2. A network lifetime (NLT) analysis of the IMEAC-DEP technique with other techniques under distinct number of nodes is provided. The experimental values denoted that the IMEAC-DEP technique has attained a higher NLT over the other methods. For instance, with 200 nodes, the IMEAC-DEP technique has achieved a maximum NLT of 18783 rounds whereas the KHO-C, GWO-C, and GOA-C techniques have offered a minimum NLT of 12840, 14977, and 17869 rounds respectively. Simultaneously, with 1000 nodes, the IMEAC-DEP technique has realized an increased NLT of 24215 rounds whereas the KHO-C, GWO-C, and GOA-C techniques have offered a minimum NLT of 20326, 21141, and 23067 rounds respectively. An analysis of the proposed IMEAC-DEP with compared methods interms of TEC is given. The experimental values depicted that the IMEAC-DEP technique has achieved improved performance with the minimum TEC. For instance, with 200 nodes, the IMEAC-DEP technique has accomplished a reduced TEC of 7.710 J whereas the KHO-C, GWO-C, and GOA-C techniques have presented an increased TEC of 12.040, 11.030, and 09.530 J respectively. Concurrently, with 1000 nodes, the IMEAC-DEP technique has got a least TEC of 14.712 J whereas the KHO-C, GWO-C, and GOA-C techniques have resulted in a raised TEC of 22.620 , 20.520, and 16.800 J respectively.

A throughput analysis of the IMEAC-DEP technique with other methods under distinct number of nodes denoted that the IMEAC-DEP technique has attained a superior throughput over the other methods. For instance, with 200 nodes, the IMEAC-DEP technique has achieved a maximal throughput of 86.430 Kbps whereas the KHO-C, GWO-C, and GOA-C techniques have offered a minimum throughput of 41.260,

53.730, and 62.230 Kbps respectively. Simultaneously, with 1000 nodes, the IMEAC-DEP method has realized an increased throughput of 94.010Kbps whereas the KHO-C, GWO-C, and GOA-C approaches have offered a minimal throughput of 61.460, 68.830, and 78.300 Kbps respectively.

Table 2: Result analysis of the IMEAC-DEP technique with existing methods

Network lifetime (Rounds)				
Number of nodes	**KHO-C**	**GWO-C**	**GOA-C**	**IMEAC-DEP**
200	12840	14977	17869	18783
400	13417	15240	18767	19880
600	15639	16923	19197	21230
800	17789	19286	21441	23685
1000	20326	21141	23067	24215
Total energy consumption (J)				
Number of nodes	**KHO-C**	**GWO-C**	**GOA-C**	**IMEAC-DEP**
200	12.040	11.030	09.530	07.710
400	15.160	11.670	09.920	08.901
600	18.870	16.260	13.000	10.947
800	21.290	19.840	16.240	11.979
1000	22.620	20.520	16.800	14.712
Throughput (Kbps)				
Number of nodes	**KHO-C**	**GWO-C**	**GOA-C**	**IMEAC-DEP**
200	41.260	53.730	62.230	86.430
400	48.630	58.330	67.830	84.670
600	52.700	62.210	70.460	90.120
800	57.170	66.730	76.140	92.460
1000	61.460	68.830	78.300	94.010

An analysis of the projected IMEAC-DEP with compared methods with respect to ETE delay is given in Fig. 2. The experimental values outperformed that the IMEAC-DEP technique has attained higher performance with the minimal ETE delay. For sample, with 200 nodes, the IMEAC-DEP approach has accomplished a minimum ETE delay of 1.936 s whereas the KHO-C, GWO-C, and GOA-C approaches have presented an increased ETE delay of 4.258, 3.014, and 2.451 s correspondingly. In line with, with 1000 nodes, the IMEAC-DEP technique has got a least ETE delay of 6.696 s whereas the KHO-C, GWO-C, and GOA-C methods have resulted in a raised ETE delay of 15.265, 12.740, and 9.501 s respectively.

A PDR analysis of the IMEAC-DEP method with other algorithms under different number of nodes is provided in Fig. 3. The experimental values referred that the IMEAC-DEP manner has attained a superior PDR over the other methods. For instance, with 200 nodes, the IMEAC-DEP technique has achieved a maximum PDR of 0.950% whereas the KHO-C, GWO-C, and GOA-C techniques have offered a minimal PDR of 0.870%, 0.900%, and 0.920% respectively. Along with this, with 1000 nodes, the

IMEAC-DEP technique has realized an increased PDR of 0.810% whereas the KHO-C, GWO-C, and GOA-C methods have offered a lesser PDR of 0.530%, 0.590%, and 0.670% correspondingly. From the results analysis, it is evident that the proposed IMEAC-DEP technique has accomplished superior performance due to the SC-AFSA based data encryption with an optimal key generation process of SC using AFSA in such a way that the security can be enhanced at the CHs.

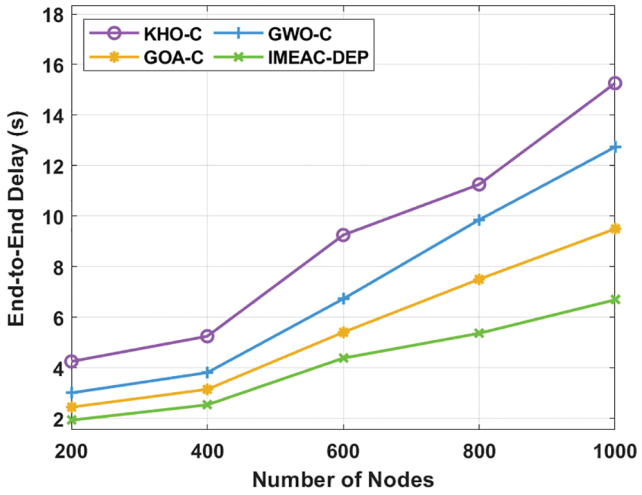

Figure 2: ETE delay analysis of IMEAC-DEP model

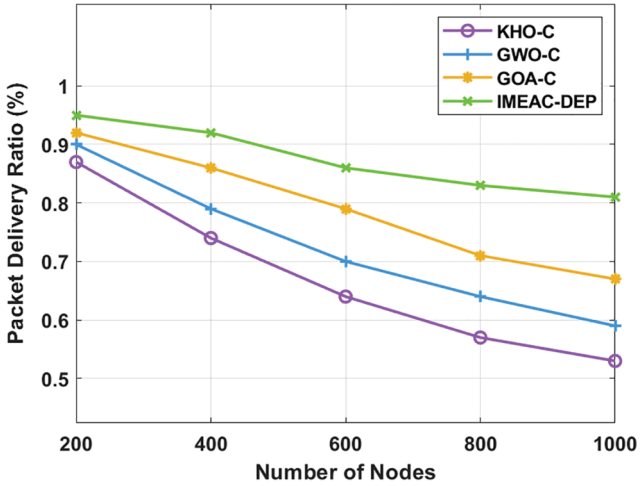

Figure 3: PDR analysis of IMEAC-DEP model with existing techniques

6 Conclusion

This paper has developed a new IMEAC-DEP model to achieve energy efficiency and secure data transmission in WSN. The IMEAC-DEP technique employs COA-C technique with four fitness parameters for optimal selection of CHs and construction of clusters. In addition, a new SC-AFSA based data encryption technique is derived, which is executed by the CHs for secured intercluster communication. The SC-AFSA technique includes an optimal key generation process of SC using AFSA in such a way that the security can be enhanced at the CHs. For examining the enhanced outcome of the

proposed IMEAC-DEP model, an extensive set of simulations take place and the results are examined interms of different measures. The resultant experimental values highlighted the superior performance of the IMEAC-DEP model over the recent stage of art methods interms of energy efficiency as well as security. In future, secure multihop routing protocol using metaheuristic optimization algorithms with trust based schemes can be developed to achieve improved security and energy efficiency.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Rawat, K. D. Singh, H. Chaouchi and J. M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *The Journal of Supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[2] M. El_Saadawy and E. Shaaban, "Enhancing S-LEACH security for wireless sensor networks," in *2012 IEEE Int. Conf. on Electro/Information Technology*, Indianapolis, IN, USA, pp. 1–6, 2012.

[3] U. Palani, V. Alamelumangai and A. Nachiappan, "Hybrid routing and load balancing protocol for wireless sensor network," *Wireless Networks*, vol. 22, no. 8, pp. 2659–2666, 2016.

[4] Z. Wang, L. Zhang, Z. Zheng and J. Wang, "Energy balancing RPL protocol with multipath for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 11, no. 5, pp. 1085–1100, 2018.

[5] C. Sureshkumar and S. Sabena, "Fuzzy-based secure authentication and clustering algorithm for improving the energy efficiency in wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1517–1536, 2020.

[6] S. Zakariayi and S. Babaie, "DEHCIC: A distributed energy-aware hexagon based clustering algorithm to improve coverage in wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 4, pp. 689–704, 2019.

[7] R. Azarderskhsh and A. Reyhani-Masoleh, "Secure clustering and symmetric key establishment in heterogeneous wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, pp. 893592, 2011.

[8] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of the 9th ACM Conf. on Computer and Communications Security*, Washington, DC USA, pp. 41–47, 2002.

[9] T. T. Nguyen, J. S. Pan and T. K. Dao, "A compact bat algorithm for unequal clustering in wireless sensor networks," *Applied Sciences*, vol. 9, no. 10, pp. 1973, 2019.

[10] J. Wang, Y. Gao, W. Liu, A. Sangaiah and H. J. Kim, "An improved routing schema with special clustering using PSO algorithm for heterogeneous wireless sensor network," *Sensors*, vol. 19, no. 3, pp. 671, 2019.

[11] T. Ahmad, M. Haque and A. M. Khan, "An energy-efficient cluster head selection using artificial bees colony optimization for wireless sensor networks," in *Advances in Nature-Inspired Computing and Applications*, Springer, Cham, pp. 189–203, 2019.

[12] M. Kumar and A. Chaparala, "OBC-WOA: Opposition-based chaotic whale optimization algorithm for energy efficient clustering in wireless sensor network," *International Journal of Intelligent Engineering & Systems*, vol. 12, no. 6, pp. 249–258, 2019.

[13] D. Chandirasekaran and T. Jayabarathi, "Cat swarm algorithm in wireless sensor networks for optimized cluster head selection: A real time approach," *Cluster Computing*, vol. 22, no. S5, pp. 11351–11361, 2019.

[14] B. Solaiman, "Energy optimization in wireless sensor networks using a hybrid k-means PSO clustering algorithm," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 24, no. 4, pp. 2679–2695, 2016.

[15] Y. Zhou, N. Wang and W. Xiang, "Clustering hierarchy protocol in wireless sensor networks using an improved PSO algorithm," *IEEE Access*, vol. 5, pp. 2241–2253, 2017.

[16] B. Baranidharan and B. Santhi, "DUCF: Distributed load balancing unequal clustering in wireless sensor networks using fuzzy approach," *Applied Soft Computing*, vol. 40, no. 4, pp. 495–506, 2016.

[17] H. Cheng, Z. Su, N. Xiong and Y. Xiao, "Energy-efficient node scheduling algorithms for wireless sensor networks using markov random field model," *Information Sciences*, vol. 329, no. 1, pp. 461–477, 2016.

[18] S. Athmani, A. Bilami and D. E. Boubiche, "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs," *Future Generation Computer Systems*, vol. 92, no. 2, pp. 789–799, 2019.

[19] J. Zhou and Z. Lin, "Lightweight load-balanced and authentication scheme for a cluster-based wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 17, no. 2, pp. 155014772098032, 2021.

[20] Z. Cui, X. U. E. Fei, S. Zhang, X. Cai, Y. Cao *et al.,* "A hybrid blockchain-based identity authentication scheme for Multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 1, 2020.

[21] N. Goyal, M. Dave and A. K. Verma, "SAPDA: Secure authentication with protected data aggregation scheme for improving QoS in scalable and survivable UWSNs," *Wireless Personal Communications*, vol. 113, no. 1, pp. 1–15, 2020.

[22] D. Guo, N. Zhang, Y. Wang, Y. Cui, B. Jiang *et al.,* "Research on information security defense based on improved identity-based dynamic clustering authentication algorithm," *Journal of Physics: Conference Series*, vol. 1757, no. 1, pp. 12136, 2021.

[23] C. Sureshkumar and S. Sabena, "Fuzzy-based secure authentication and clustering algorithm for improving the energy efficiency in wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1517–1536, 2020.

[24] G. I. L. and V. Kavitha, "Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 821–836, 2021.

[25] S. Arjunan and P. Sujatha, "Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol," *Applied Intelligence*, vol. 48, no. 8, pp. 2229–2246, 2018.

[26] M. Khishe and M. R. Mosavi, "Chimp optimization algorithm," *Expert Systems with Applications*, vol. 149, pp. 113338, 2020.

[27] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja and K. S. Kumar, "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization," in *Cybersecurity and Secure Information Systems*, Springer, Cham, pp. 31–42, 2019.

[28] Q. He, X. Hu, H. Ren and H. Zhang, "A novel artificial fish swarm algorithm for solving large-scale reliability-redundancy application problem," *ISA Transactions*, vol. 59, no. 2, pp. 105–113, 2015.

[29] P. Manickam, K. Shankar, E. Perumal, M. Ilayaraja and K. S. Kumar, "Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography," in *Cybersecurity and Secure Information Systems*, Springer International Publishing, New York, US, pp. 193–204, 2019.