Computers, Materials & Continua
DOI: 10.32604/cmc.2022.031660
Article

Tech Science Press

Chaotic Pigeon Inspired Optimization Technique for Clustered Wireless Sensor Networks

Anwer Mustafa Hilal[1,2,*], Aisha Hassan Abdalla Hashim[1], Sami Dhahbi[3], Dalia H. Elkamchouchi[4], Jaber S. Alzahrani[5], Mrim M. Alnfiai[6], Amira Sayed A. Aziz[7] and Abdelwahed Motwakel[2]

[1]Department of Electrical and Computer Engineering, International Islamic University Malaysia, 53100, Kuala Lumpur, Malaysia
[2]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
[3]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
[5]Department of Industrial Engineering, College of Engineering at Alqunfudah, Umm Al-Qura University, Saudi Arabia
[6]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, P.O. Box 11099, Taif, 21944, Saudi Arabia
[7]Department of Digital Media, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo, 11835, Egypt
*Corresponding Author: Anwer Mustafa Hilal. Email: a.hilal@psau.edu.sa
Received: 23 April 2022; Accepted: 08 June 2022

Abstract: Wireless Sensor Networks (WSN) interlink numerous Sensor Nodes (SN) to support Internet of Things (loT) services. But the data gathered from SNs can be divulged, tempered, and forged. Conventional WSN data processes manage the data in a centralized format at terminal gadgets. These devices are prone to attacks and the security of systems can get compromised. Blockchain is a distributed and decentralized technique that has the ability to handle security issues in WSN. The security issues include transactions that may be copied and spread across numerous nodes in a peer-peer network system. This breaches the mutual trust and allows data immutability which in turn permits the network to go on. At some instances, few nodes die or get compromised due to heavy power utilization. The current article develops an Energy Aware Chaotic Pigeon Inspired Optimization based Clustering scheme for Blockchain assisted WSN technique abbreviated as EACPIO-CB technique. The primary objective of the proposed EACPIO-CB model is to proficiently group the sensor nodes into clusters and exploit Blockchain (BC) for inter-cluster communication in the network. To select Cluster Heads (CHs) and organize the clusters, the presented EACPIO-CB model designs a fitness function that involves distinct input parameters. Further, BC technology enables the communication between one CH and the other and with the Base Station (BS) in the network. The authors conducted comprehensive set of simulations and the outcomes were investigated under different aspects. The

simulation results confirmed the better performance of EACPIO-CB method over recent methodologies.

Keywords: Blockchain; wireless sensor networks; clustering; energy efficiency; security; data transmission

1 Introduction

Wireless Sensor Network (WSN) encompasses multiple technologies into it such as wireless communication, sensing, and computing [1]. In general, the external targets are observed literally via several kinds of microsensors. These microsensors generate a vast amount of sensitive information at an unexpected rate. Even though it is common to have distinct application phenomenon and hardware positioning, the utmost objective is to collect, transmit and process the collected data. At last, the end users get intriguing information from the data source [2].

Since WSN is regarded as a data-centric network system, it has a basic issue to be resolved i.e., data storage of nodes in WSN [3]. The users are highly concerned about the perception of data than the Sensor Node (SN) and the networks it is made up of. Moreover, WSN system helps in dependable and effective data storage and accessibility over a variety of atmospheres that are mostly unreliable. Storage level and energy consumption of every SN are restricted up to certain limit. So, efficient data storage under storage constraints has become a significant research area in WSN data management. Fig. 1 illustrates the structure of blockchain in WSN.

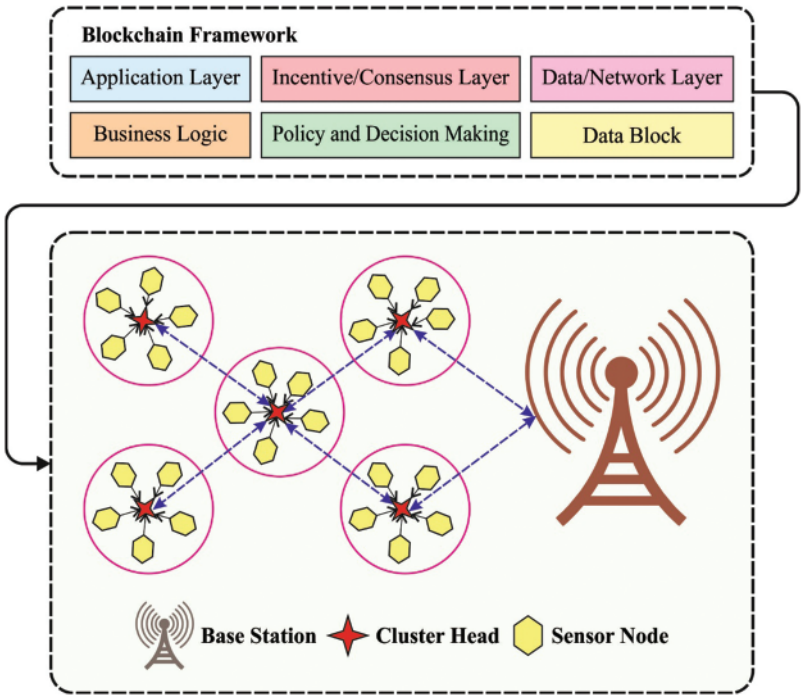

Figure 1: Blockchain in WSN

Clustering is a main technique applied in achieving lengthy network lifespan. In this process, the sensors are grouped into groups of clusters while a leader i.e., Cluster Head (CH) is selected for every

group [4]. Data aggregation, in connection with Compressive Sensing (CS), is different from other approaches since the key objective is to minimize data communication and attain superior power efficiency. In the study conducted earlier [5], Plain-CS was positioned with random sparse projection and hybrid-CS so as to restrict the energy consumption of sensors to a large extent. These models are appropriate for minimizing complete network communication cost. On the other hand, it also recognizes the grouping of routing principles which possesses data aggregation characteristics that tend to increase network's effectiveness [6]. This method considers 'power efficiency' as a basic demand due to power restraints in nodes. Afterwards, minimizing energy consumption and sustaining power efficacy are considered as important problems.

Security menace is one of the most important problems found in WSNs. Since SNs have resource-constraints, they are prone to attacks in a simple manner [7]. In general, WSNs face two kinds of attacks such as physical attacks and internal attacks. In physical attacks, the aggressors have full control over the SNs to perform malevolent actions. In case of internal attacks, SNs act in a selfish manner to preserve its power and memory. So, it becomes highly essential to recognize and eradicate the malignant sensors from the network [8]. Blockchain (BC) technology is the only choice to resolve these problems as discussed above. In this technique, smart contracts are presented in which every agreement is framed in the system. It is an efficient method to maintain a database of transactions amongst various groups [9]. As BC is unchallengeable, it is not possible to tamper the data. In BC, the transaction data remains safe since the blocks are connected by hashes [10].

Sanchez et al. [11] projected a decentralized model to ensure both autonomy and security of IoT model. The presented technique can be utilized for the protection of data integrity and accessibility based on the security benefits provided by BC technique and by using cryptographic tools. The accuracy of the presented technique was evaluated on temperature and humidity sensors on Internet of Things (IoT)-based WSN. She et al. [12] examined a BC Trust Model (BTM) for malicious node detection in WSNs. Primarily, the proposed model offers the entire structure of the trust model. Next, it generates the BC data structure that is utilized in the detection of malicious nodes. At last, it recognizes the malicious nodes from 3D space with the help of BC smart contracts and WSN quadrilateral measurement localization approach.

In the study conducted earlier [13], a BC-based decentralized structure was established in combination with authentication and privacy preserving methods to secure data transmission from WSN-allowed IoTs. Registration, certification, and revocation procedures were utilized for the transmission of data between SN and Base Station (BS) in Cloud Computing (CC) environment. In literature [14], a novel effectual authentication method was proposed for WSNs using BC technique so as to accomplish security. The nodes, present in WSNs, form the IoT network which are expressed as BS, CHs, and normal SN. The structure of a BC network is shaped by a hierarchical BC method that contains small chain and global chain amongst many network nodes. Rahman et al. [15–17] established a layered hierarchical structure to be utilized upon distributed-yet-effectual BC-allowed SDN-IoT structure. This structure ensures effective CH selection and secure network transmission using identification and isolation of rouge switches.

The current study develops an Energy Aware Chaotic Pigeon Inspired Optimization based Clustering Scheme for Blockchain Assisted WSN abbreviated as EACPIO-CB technique. The primary intention of the proposed EACPIO-CB model is to proficiently group the SNs into clusters and exploit BC for inter-cluster communication in the network. To select the CHs and organize the clusters, the presented EACPIO-CB model designs a Fitness Function (FF) with distinct input parameters. In addition, BC technology enables communication between one CH and the other and with the BS

in the network. The researchers conducted comprehensive set of simulations and the outcomes were examined under different aspects.

Rest of the study is planned as follows. Section 2 elaborates the proposed model and Section 3 validates the performance of the proposed model. At last, Section 4 draws the concluding remarks.

2 Design of EACPIO-CB Model

In this article, a new EACPIO-CB method has been developed to attain security and energy efficiency in WSN. The aim of the proposed EACPIO-CB model is to proficiently group the SNs into clusters and exploit BC for inter-cluster communication in the network. Fig. 2 showcases the block diagram of EACPIO-CB technique.

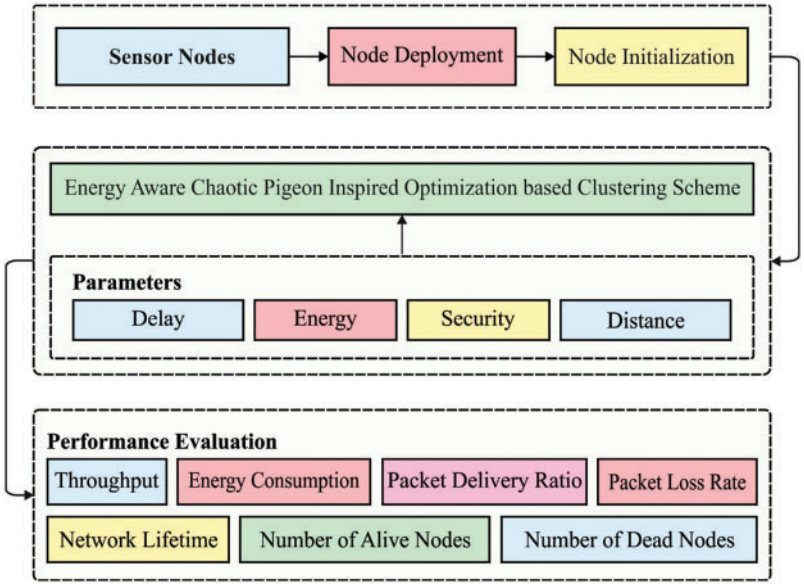

Figure 2: Overall block diagram of EACPIO-CB technique

2.1 Overview of CPIO Algorithm

PIO approach is a meta-heuristic algorithm that is simulated based on pigeon returning behaviour [18]. The pigeon detects its nest with elements that support its returning such as magnetic field, sun, and landmarks. It can affect the path of entire population. Then, the nearby landmarks assist the pigeons to fly nearby the end of the path. In order to mimic the natural activity of pigeons returning to nest, PIO approach employs two operatives to describe the clustering nature of pigeons. In PIO mode, compass and map operators from the primary stage signify the impact of magnetic field and sun once the landmark operators, in the resulting stage, outline the effect of landmarks on returning home.

When the entire flock is initiated, the amount of pigeons is denoted by N_p, the activity dimension is characterized by D_{im}, compass and map features are denoted by R, and the location and speed of pigeons are characterized based on the following equations.

$$Pos_i = \left[Pos_{i1}, Pos_{i2}, \cdots Pos_{iD_i m}\right] \tag{1}$$

$$Vel_i = \left[Vel_{i1}, Vel_{i2}, \cdots Vel_{iD_i m}\right] \tag{2}$$

During compass and map operators phase, the entire pigeon population provides a strong global searching ability which professionally prevents the solution from falling into local optima issue.

The original position and the speed of the flock to upgrade the line of attack are as follows.

$$Pos_i^{t+1} = Pos_i^t + Vel_k^{t+1} \tag{3}$$

$$Vel_i^{t+1} = e^{-R*t} * Vel_i^t + \phi_1 * \left(Pos_{gbest} - Pos_i\right) \tag{4}$$

In the abovementioned equation, Pos_{gbest} indicates the position of pigeon with optimal fitness value in the entire population after every upgrade, t represents the number of iterations for the whole population, and ϕ_1 characterizes the variable constrained from [0,1].

$$Vel^{t+1} = w * Vel_t + c1 * rand(0,1)\ (P_{best} - Pos) + c2 * rand(0,1)\ (G_{best} - Pos) \tag{5}$$

Eq. (5) shows the velocity update formula of Particle Swarm Optimization (PSO) model i.e., the migrant direction of the swarming bird. Eq. (4) is the speed upgrading formula for PIO which simulates the home returning nature of pigeons. The upgraded formula for speed is given in the first stage [19]. In comparison with PSO algorithm, no individual optimal effects exist while there is a strong global searching ability available for the prevention of problems of falling under local optima.

Initially, the population needs to eliminate the pigeons that do not have a direction which they can recognize. Further, the population also should consider the pigeons that prevent them from influencing the iteration path of population as represented in the equation given below. Then, the pigeon is selected based on each leadership from the population as represented in the following equation. At last, the pigeon that results from the entire population is repeated as follows.

$$N_p^t = \frac{N_p^{t-1}}{2} \tag{6}$$

$$Pos_{center}^t = \frac{\Sigma_{i=1}^{N_p^t} Pos_i^t * F(Pos_i^t)}{N_p^t * \Sigma_{i=1}^{N_p^t} F\left(Pos_i^t\right)} \tag{7}$$

$$Pos_i^{t+1} = Pos_i^t + \phi_4 * (Pos_{center}^t - Pos_i^t) \tag{8}$$

In this equation, $F\left(Pos_i^t\right)$ symbolizes the process of fitness value solution. When the function needs minimal and maximal values, it contains dissimilar terms as represented below. Here, ε indicates an arbitrary constant that prevents $F\left(Pos_i^t\right)$ from falling into 0.

$$F\left(Pos_i^t\right) = \begin{cases} fitness\ \left(Pos_i^t\right)\ for\ maximization\ problem \\ \dfrac{1}{f^{fitness\left(Pos_i^t\right)+\varepsilon}} for\ minimization\ problem \end{cases} \tag{9}$$

In order to enhance the efficacy of PIO approach, chaotic dynamics are integrated to derive the CPIO technique. Because it offers a uniform distribution within [0,1] while the tent mapping illustrates high advantages and heavy iterative speed than the logistic mapping process [20]. Tent map is used to calculate the dynamical systems, since it has different characteristics like simple shape, chaotic orbits, etc. Here, tent mapping is applied to generate the chaos parameter while the tent map can be defined as given below.

$$z_{n+1} = \mu\left(1 - 2\left|z_n - 0.5\right|\right), 0 \le z_0 \le 1, n = 0, 1, 2, \ldots, \tag{10}$$

Here, $u \in (0,1)$ indicates the bifurcation parameter. Especially, if $\mu = 1$, the tent mapping establishes ergodicity and chaotic dynamics within [0,1]. Two chaos sequences are disseminated after many iterations with earlier point in 2D space. Chaotic dynamic is applied to initiate and is determined in the following equation. With tent mapping $(\mu = 1)$, the chaos variable is attained using the following equation.

$$z_{\mathrm{j}}^{(\mathrm{i}+1)} = \mu\left(1 - 2\left|z_j^{(i)} - 0.5\right|\right), \quad \mathrm{j} = 1, 2, \cdots, D, \tag{11}$$

Here, z_j characterizes j th dimension and i shows the iteration count. The value $i = 0$ is a fixed one while D variables are generated using the equation given above. Then, consider $\mathrm{i} = 1, 2, \ldots, \mathrm{N}$ in a sequential order and generate the most important swarm. Subsequently, the chaos variable through $z_j^{(i)}$, $\mathrm{i} = 1, 2, \ldots, N$ is mapped with the searching extent of variable decision.

$$\mathrm{x}_{ij} = \mathrm{x}_{\min,\,\mathrm{j}} + z_{\mathrm{j}}^{(\mathrm{i})}\left(\mathrm{x}_{\max,\,\mathrm{j}} - \mathrm{x}_{\min,\,\mathrm{j}}\right), \mathrm{j} = 1, 2, \ldots, \mathrm{D}. \tag{12}$$

$$\mathrm{x}_i = \left(\mathrm{x}_{i1}, \mathrm{x}_{i2}, \ldots, \mathrm{x}_{iD}\right), \; i = 1, 2, \ldots, N, \tag{13}$$

Chaotic map initiates the swarming of PIO. According to chaotic searching process, chaotic disturbance encompassess

$$z' = (1 - \gamma)\,\psi^* + \gamma z, \tag{14}$$

Here, γ characterizes the parameters that fall into [0,1], $z' = \left(z_1', z_2', \ldots, z_D'\right)$ indicates the chaos vector after the addition of disturbance. ψ^* designates the optimal chaos vector, once the existing optimal $\mathrm{x}^* = \left(\mathrm{x}_1^*, \mathrm{x}_2^*, \ldots, \mathrm{x}_D^*\right)$ is mapped towards [0,1]:

$$\psi^* = \frac{x^* - x_{min}}{x_{max} - x_{min}}. \tag{15}$$

2.2 *Processes Involved in EACPIO-CB Model*

The presented EACPIO-CB model designs a FF involving distinct input parameters. The main concept of the proposed EACPIO-CB algorithm on CH selection is to decrease the distance between the selected nodes and CH. Further, it also focuses on reducing the timeline delay to transmit the information from one node to another. On the contrary, network energy has to be higher, i.e., during data transmission, it needs to employ a small amount of energy. At last, the node must tolerate the risks present in the network. The objective function of the adapted CH is demonstrated using Eq. (16), while the value of η should depend upon $0 < \eta < 1$. Now, v_m and v_n indicate the operations as demonstrated in Eqs. (17) and (18). The constraint on energy, delay, security, and distance are denoted by σ_1, σ_2, σ_3 and σ_4. The condition of this constraint is specified by, $\sigma_1 + \sigma_2 + \sigma_3 + \sigma_4 = 1$. $Y^Z - S_s$ represents the distance between normal and sink nodes.

$$N_n = \eta v_n + (1 - \eta)\, v_m \tag{16}$$

$$v_m = \sigma_1 * v_i^{dis} + \sigma_2 * v_{i^{me}} + \sigma_3 * v_{i^{de/}} + \sigma_4 * v_{i\,\mathrm{sec}} \tag{17}$$

$$v_n = \frac{1}{b}\sum\nolimits_{z=1}^{b} \| Y^K - S_J \| \tag{18}$$

Eq. (19) portrays the FF for distance wherein *l*) $di_J\,(m)$ is related to packet transmission from average node to CH and from CH to *BS*. Generally v_{idis} ranges from [0, 1] and the values go high, when the distance amongst the average node and CH is higher. Eqs. (20) and (21) correspondingly depict $v_{(m)}^{dis}$ and $v^{dis}\,(n)$, where Y_z represents the normal node in zth cluster, G_z describes the CH of Z^{th} cluster, the distance between BS and CH is characterized by $G_Z - S_s$, $G_Z - Y_y$ signifies the distance between the CH and average node and $Y_z - Y_y$ refers to the distance between two average nodes and M_z and $M_y\vee$ indicate the number of nodes excluding Z^{th} and yth clusters.

$$v_i^{dis} = \frac{v_{(m)}^{dis}}{v_{(n)}^{dis}} \tag{19}$$

$$v_{(m)}^{dis} = \sum_{z=1}^{M_z}\left[||G_x - S_s|| + \sum_{y=1}^{M_y}\|G_Z - Y_y\|\right] \tag{20}$$

$$v_{(n)}^{dis} = \sum_{z=1}^{M_z}\sum_{y=1}^{M_y}\|Y_Z - Y_y\| \tag{21}$$

Eq. (22) details about the FF of energy. The value v_{iene} is greater than one and the whole CH cumulative $v_{(m)}^{ene}$ and $v_{(n)}^{ene}$ is concerned with maximum energy value and high amount of CH.

$$v_i^{ene} = \frac{v_{(m)}^{ene}}{v_{(n)}^{ene}} \tag{22}$$

The FF of delay v_i^{del} that lies within [0, 1] is depicted in Eq. (23). v_i^{del} is equivalent to each node that resides in a cluster. Thus, the delay gets reduced, when CH has a minimum number of nodes. The denominator M_M indicates the overall node count in WSN, and the numerator denotes the high CH count.

$$v_i^{del} = \frac{\max\left(\|G_z - Y_z\|\right)_{z=1}^{M_c}}{M_M} \tag{23}$$

2.3 BC Enabled Inter-Cluster Communication

In this work, BC technology enables communication between one CH and the other and between one CH and BS in the network. In general, BC is hypothesized as a group of blocks; and those blocks contain hash values of the existing blocks, dataset about the transaction (Ethereum, bitcoin), timestamp, and previous block. Furthermore, BC is determined by a common and distributed digital ledger that is employed to store the transaction data under different points. Thus, when attackers attempt to acquire the dataset, it is not possible for them to do so, since each and every block has a cryptographic value of the preceding block. Now, each transaction is performed under the application of cryptographic hash values i.e., confirmed by all the miners. It is taken by the same value of a comprehensive ledger and is encompassed by the block of each transaction. BC offers the capability to share the ledger information in a protective, shared, and private manner. Decentralized storage is an alternative method offered by BC in which huge volumes of information are linked and stored from the present blocks to preceding blocks using a smart contract code. LitecoinDB, Swarm, Interplanetary File System (IPFS), MoneroDB, SiacoinDB, BigchainDB, etc., are employed for decentralized datasets.

3 Results and Discussion

The current section deals with experimental validation of the proposed EACPIO-CB model under distinct aspects. Tab. 1 and Fig. 3 shows the PDR analysis results achieved by the proposed EACPIO-CB approach and other recent models such as Red Deer Algorithm (RDA), Genetic Algorithm (GA), Ant Lion Algorithm (ALO), Grey Wolf Algorithm (GWO) and PSO [21]. The results highlight that the proposed EACPIO-CB approach accomplished enhanced PDR values under different number of SNs. For sample, with 100 SNs, the proposed EACPIO-CB model offered a high PDR of 99.43%, while RDA, GA, ALO, GWO, and PSO systems obtained low PDR values such as 97.82%, 96.23%, 94.82%, 93.32%, and 91.07% respectively. Moreover, with 500 SNs, the proposed EACPIO-CB model offered a high PDR of 97.24%, while RDA, GA, ALO, GWO, and PSO methodologies achieved low PDR values such as 96.37%, 94.70%, 92.60%, 90.32%, and 89.42% correspondingly.

Table 1: PDR analysis results of EACPIO-CB algorithm and other existing approaches under distinct number of SNs

Packet delivery ratio (%)						
Sensor nodes	EACPIO-CB	Red deer algorithm	Genetic algorithm	Ant lion algorithm	Grey wolf algorithm	Particle swarm algorithm
100	99.43	97.82	96.23	94.82	93.32	91.07
200	99.29	97.96	95.85	93.69	92.22	90.78
300	99.11	97.38	95.85	93.26	91.85	90.63
400	97.96	96.66	95.25	92.80	90.66	89.62
500	97.24	96.37	94.70	92.60	90.32	89.42

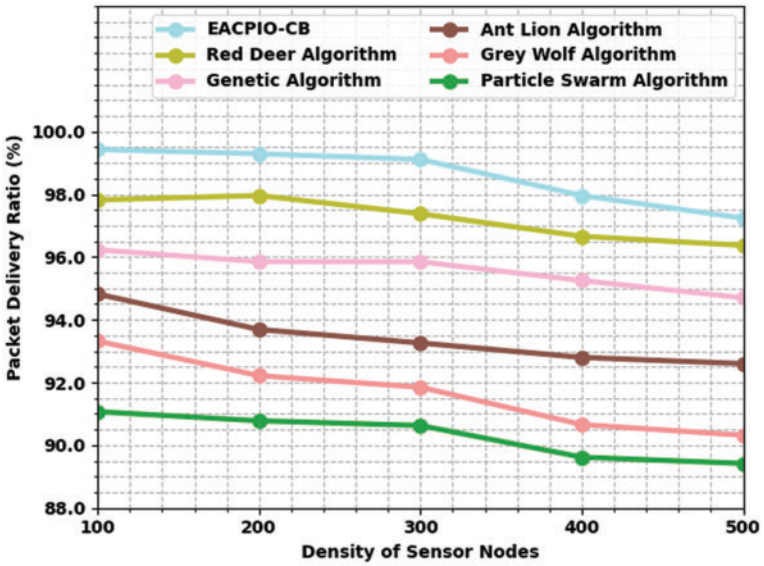

Figure 3: PDR analysis results of EACPIO-CB technique under distinct number of SNs

Comparative Packet Loss Rate (PLR) analysis was conducted between EACPIO-CB model and other existing models and the results are shown in Tab. 2 and Fig. 4. The experimental outcomes imply that the proposed EACPIO-CB technique produced effectual outcomes with low PLR values under all the instances. For instance, with 100 SNs, the proposed EACPIO-CB system attained a minimal PLR of 0.57%, whereas RDA, GA, ALO, GWO, and PSO models demonstrated maximum PLR values such as 2.18%, 3.77%, 5.18%, 6.68%, and 8.93% correspondingly. Also, with 500 SNs, the proposed EACPIO-CB system depicted a minimal PLR of 2.76%, whereas RDA, GA, ALO, GWO, and PSO techniques established maximum PLR values such as 3.63%, 5.30%, 7.40%, 9.68%, and 10.58% correspondingly.

Table 2: PLR analysis results of EACPIO-CB algorithm and other existing approaches under distinct number of SNs

Packet loss rate (%)						
Sensor nodes	EACPIO-CB	Red deer algorithm	Genetic algorithm	Ant lion algorithm	Grey wolf algorithm	Particle swarm algorithm
100	0.57	2.18	3.77	5.18	6.68	8.93
200	0.71	2.04	4.15	6.31	7.78	9.22
300	0.89	2.62	4.15	6.74	8.15	9.37
400	2.04	3.34	4.75	7.20	9.34	10.38
500	2.76	3.63	5.30	7.40	9.68	10.58

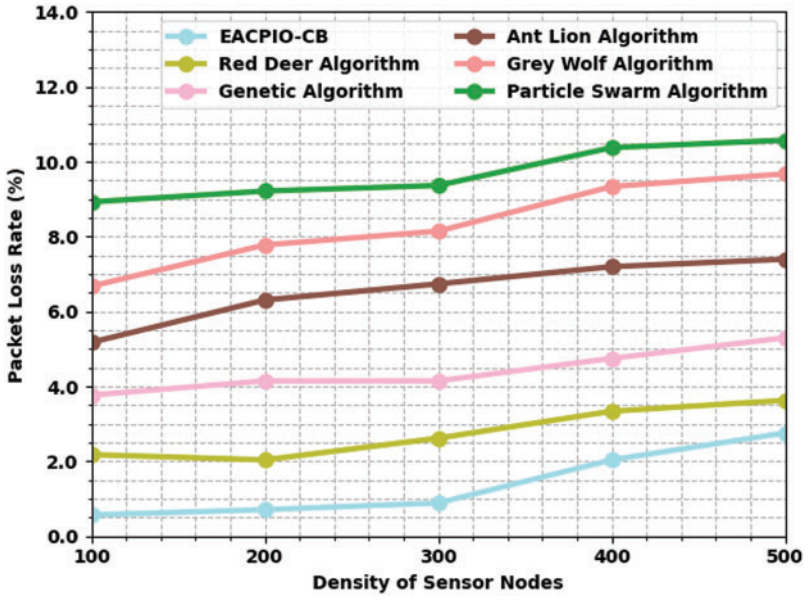

Figure 4: PLR analysis results of EACPIO-CB algorithm under different number of SNs

Tab. 3 and Fig. 5 shows the Throughput (THPT) examination results attained by the proposed EACPIO-CB method and other recent methodologies. The results highlight that EACPIO-CB approach accomplished high THPT values under distinct number of SNs. For instance, with 100 SNs, the proposed EACPIO-CB model offered a high THPT of 98.35%, while RDA, GA, ALO, GWO, and PSO systems obtained the least THPT values such as 89.92%, 86.55%, 79.39%, 74.54%, and 53.26% respectively. Eventually, with 500 SNs, the presented EACPIO-CB method offered an increased THPT of 81.92%, whereas RDA, GA, ALO, GWO, and PSO algorithms obtained minimal THPT values such as 71.80%, 61.90%, 47.15%, 38.30%, and 30.51% respectively.

Table 3: Throughput analysis results of EACPIO-CB technique and other existing approaches under distinct number of SNs

Throughput (%)						
Sensor nodes	EACPIO-CB	Red deer algorithm	Genetic algorithm	Ant lion algorithm	Grey wolf algorithm	Particle swarm algorithm
100	98.35	89.92	86.55	79.39	74.54	53.26
200	94.77	87.82	79.60	68.22	50.73	38.72
300	90.13	82.97	68.01	56.42	46.52	31.77
400	85.08	79.39	64.22	49.05	41.89	30.93
500	81.92	71.80	61.90	47.15	38.30	30.51

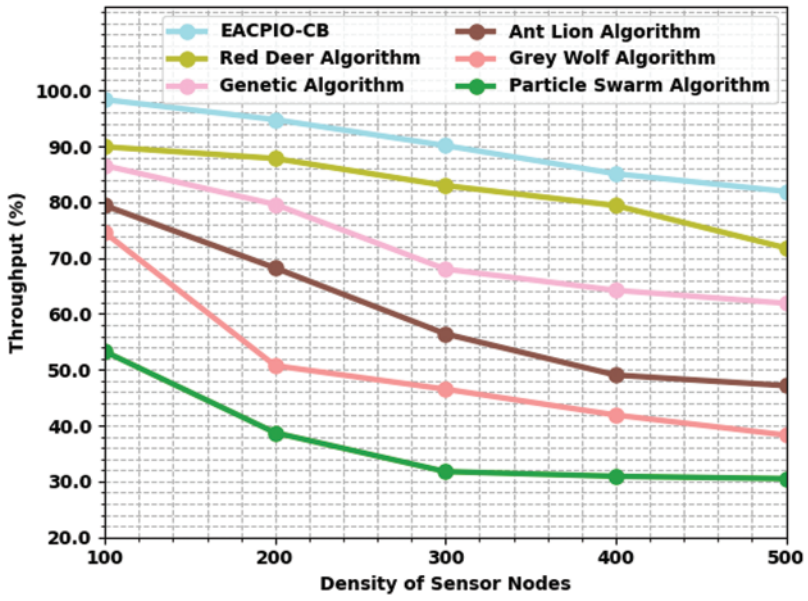

Figure 5: Throughput analysis results of EACPIO-CB algorithm under different number of SNs

Comparative Energy Consumption (ECM) investigation was conducted between EACPIO-CB method and other existing models and the results are shown in Tab. 4 and Fig. 6. The experimental

outcomes denote that the proposed EACPIO-CB model produced effectual outcomes with the least values of ECM. For instance, with 100 SNs, EACPIO-CB system achieved a low ECM of 0.02 mJ, whereas RDA, GA, ALO, GWO, and PSO models attained high ECM values such as 0.04, 0.05, 0.07, 0.09, and 0.15 mJ correspondingly. At last, with 500 SNs, the proposed EACPIO-CB method accomplished a minimum ECM of 0.34 mJ, whereas RDA, GA, ALO, GWO, and PSO models demonstrated maximum ECM values such as 0.52, 0.65, 0.79, 0.88, and 0.97 mJ correspondingly.

Table 4: ECM analysis results of EACPIO-CB technique and other existing approaches under distinct number of SNs

Energy consumption (mJ)						
Sensor nodes	EACPIO-CB	Red deer algorithm	Genetic algorithm	Ant lion algorithm	Grey wolf algorithm	Particle swarm algorithm
100	0.02	0.04	0.05	0.07	0.09	0.15
200	0.06	0.11	0.21	0.23	0.34	0.44
300	0.11	0.21	0.29	0.43	0.55	0.61
400	0.21	0.36	0.46	0.60	0.74	0.82
500	0.34	0.52	0.65	0.79	0.88	0.97

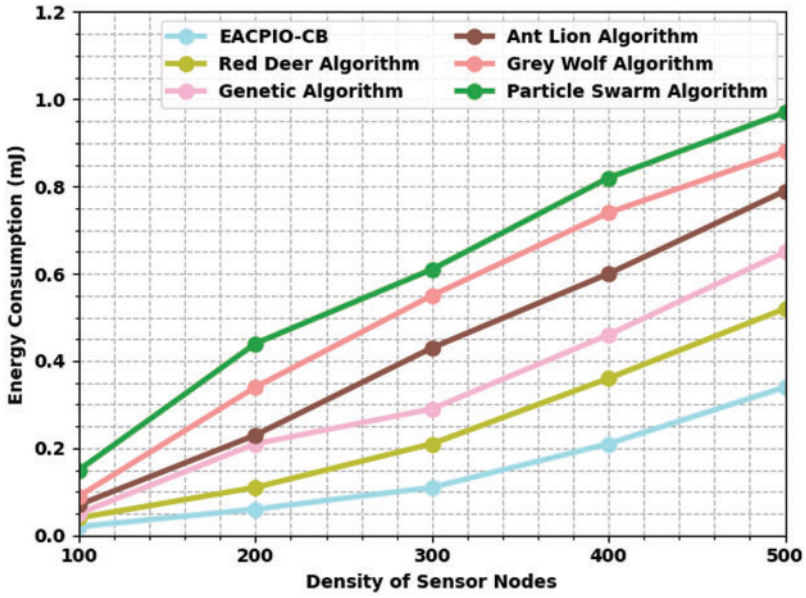

Figure 6: ECM analysis results of EACPIO-CB algorithm under different number of SNs

Tab. 5 and Fig. 7 portrays the Network Lifetime (NLT) analysis results accomplished by the proposed EACPIO-CB system and other recent models. The results highlight that the proposed EACPIO-CB system accomplished improved NLT values under different number of SNs. For sample, with 100 SNs, the proposed EACPIO-CB model offered a superior NLT of 1881 rounds, while RDA,

GA, ALO, GWO, and PSO techniques obtained lesser NLT values such as 1684, 1621, 1527, 1393, and 1280 rounds correspondingly. Likewise, with 500 SNs, the proposed EACPIO-CB model achieved a high NLT of 3920 rounds, whereas RDA, GA, ALO, GWO, and PSO methodologies obtained minimal NLT values such as 3821, 3787, 3566, 3440, and 3120 rounds correspondingly.

Table 5: NLT analysis results of EACPIO-CB technique and other existing approaches under distinct number of SNs

Network lifetime (Rounds)						
Sensor nodes	EACPIO-CB	Red deer algorithm	Genetic algorithm	Ant lion algorithm	Grey wolf algorithm	Particle swarm algorithm
100	1881	1684	1621	1527	1393	1280
200	2558	2306	2031	1905	1716	1468
300	3275	3015	2684	2543	2322	2172
400	3881	3606	3244	3118	2826	2580
500	3920	3821	3787	3566	3440	3120

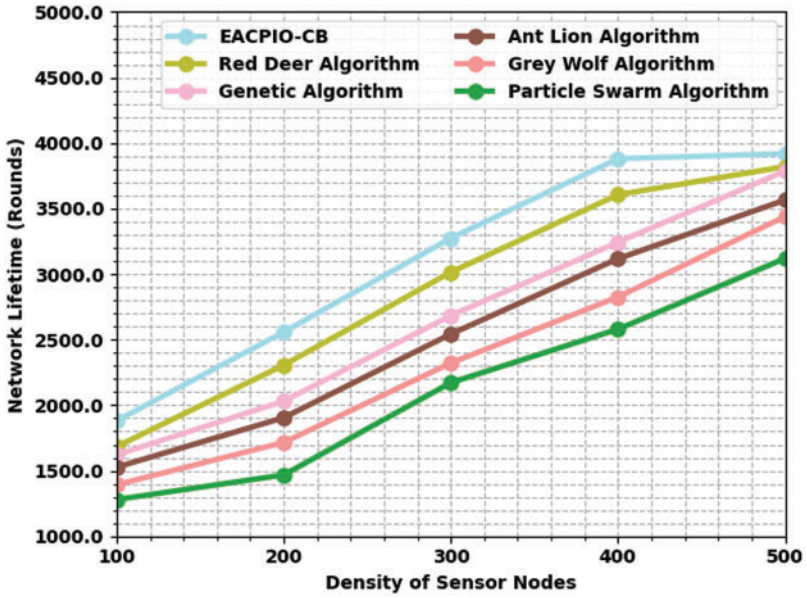

Figure 7: NLT analysis results of EACPIO-CB algorithm under distinct number of SNs

Tab. 6 shows the Number of Alive Sensor Nodes (NOASN) analysis results achieved by the proposed EACPIO-CB model and other recent techniques. The outcomes highlight that the proposed EACPIO-CB approach accomplished high NOASN values under varying number of rounds. For instance, with 400 rounds, the presented EACPIO-CB system obtained the maximum NOASN of 500, whereas RDA, GA, ALO, GWO, and PSO algorithms attained low NOASN values such as 491, 471, 430, 401, and 372 correspondingly.

Table 6: NOASN analysis results of EACPIO-CB algorithm and other existing approaches under distinct rounds

No. of alive sensor nodes						
No. of rounds	EACPIO-CB	Red deer algorithm	Genetic algorithm	Ant lion algorithm	Grey wolf algorithm	Particle swarm algorithm
0	500	500	500	500	500	500
400	500	491	471	430	401	372
800	492	486	450	416	380	356
1200	492	481	429	403	363	339
1600	491	473	417	388	347	309
2000	490	449	406	372	318	285
2400	476	420	375	326	228	188
2800	422	368	322	258	144	102
3200	341	289	251	172	38	13
3600	284	209	110	68	0	0
4000	213	124	10	0	0	0

Furthermore, with 3200 rounds, the proposed EACPIO-CB system offered a high NOASN of 341, whereas RDA, GA, ALO, GWO, and PSO algorithms obtained the least NOASN values such as 289, 251, 172, 38, and 13 correspondingly.

4 Conclusion

In current study, a novel EACPIO-CB technique has been developed to attain security and energy efficiency in WSN. The aim of the proposed EACPIO-CB model is to proficiently group the SNs into clusters and exploit BC for inter-cluster communication in the network. To choose the CHs and organize the clusters, the presented EACPIO-CB model designs an FF that involves distinct input parameters. In addition, BC technology enables communication between one CH and the other and with BS in the network. The researchers conducted a comprehensive set of simulations and the outcomes were examined under different aspects. The simulation outcomes established the superior performance of the proposed EACPIO-CB technique on recent approaches. In future, multi-hop route planning scheme can also be developed to improve energy efficiency outcomes.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project under grant number (142/43). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R238), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4340237DSR24).

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

References

[1] Z. Cui, F. Xue, 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. 241–251, 2020.

[2] 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.

[3] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Information Systems*, vol. 2018, pp. 1–10, 2018.

[4] S. Arjunan and P. Sujatha, "A survey on unequal clustering protocols in wireless sensor networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 1, pp. 118, 2021.

[5] S. Famila, A. Jawahar, A. Sariga and K. Shankar, "Improved artificial bee colony optimization based clustering algorithm for SMART sensor environments," *Peer-to-Peer Networking and Applications*, vol. 13, no. 4, pp. 1071–1079, 2020.

[6] S. Verma, S. Kaur, R. Manchanda and D. Pant, "Essence of blockchain technology in wireless sensor network: A brief study," in *2020 Int. Conf. on Advances in Computing, Communication & Materials (ICACCM)*, Dehradun, India, pp. 394–398, 2020.

[7] S. Arjunan, S. Pothula and D. Ponnurangam, "F5 N-based unequal clustering protocol (F5NUCP) for wireless sensor networks," *International Journal of Communication Systems*, vol. 31, no. 17, pp. e3811, 2018.

[8] R. C. Vara, J. Prieto and J. M. Corchado, "How blockchain could improve fraud detection in power distribution grid," in *The 13th Int. Conf. on Soft Computing Models in Industrial and Environmental Applications, Advances in Intelligent Systems and Computing Book Series*, Springer, Cham, vol. 771, pp. 67–76, 2018.

[9] S. Amjad, S. Abbas, Z. Abubaker, M. Alsharif, A. Jahid *et al.* "Blockchain based authentication and cluster head selection using DDR-leach in internet of sensor things," *Sensors*, vol. 22, no. 5, pp. 1972, 2022.

[10] D. Sivaganesan, "A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks," *Journal of Trends in Computer Science and Smart Technology (TCSST)*, vol. 3, no. 1, pp. 59–69, 2021.

[11] A. E. G. Sanchez, E. A. R. Araiza, J. L. G. Cordoba, M. T. Ayala and A. Takacs, "Blockchain mechanism and symmetric encryption in a wireless sensor network," *Sensors*, vol. 20, no. 10, pp. 2798, 2020.

[12] W. She, Q. Liu, Z. Tian, J. S. Chen, B. Wang *et al.* "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[13] R. Goyat, G. Kumar, R. Saha, M. Conti, M. K. Rai *et al.,* "Blockchain-based data storage with privacy and authentication in internet-of-things," *IEEE Internet Things Journal*, pp. 1–1, 2020, doi:10.1109/JIOT.2020.3019074.

[14] A. Mubarakali, "An efficient authentication scheme using blockchain technology for wireless sensor networks," *Wireless Personal Communications*, 2021, https://doi.org/10.1007/s11277-021-08212-w.

[15] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza *et al.,* "SmartBlock-SDN: An optimized blockchain-sdn framework for resource management in IoT," *IEEE Access*, vol. 9, pp. 28361–28376, 2021.

[16] M. A. A. Almekhlafi, T. A. Elfadil Eisa, F. N. Al-Wesabi, A. Abdelmaboud, M. A. Hamza *et al.,* "Efficiency effect of obstacle margin on line-of-sight in wireless networks," *Computers, Materials & Continua*, vol. 72, no. 1, pp. 227–242, 2022.

[17] F. N. A. Wesabi, M. Obayya, M. Hamza, J. S. Alzahrani, D. Gupta *et al.,* "Energy aware resource optimization using unified metaheuristic optimization algorithm allocation for cloud computing environment," *Sustainable Computing: Informatics and Systems*, vol. 35, 2022.

[18] H. Duan and X. Wang, "Echo state networks with orthogonal pigeon-inspired optimization for image restoration," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 11, pp. 2413–2425, 2016.
[19] Z. Cui, J. Zhang, Y. Wang, Y. Cao, X. Cai *et al.,* "A Pigeon-inspired optimization algorithm for many-objective optimization problems," *Science China Information Sciences*, vol. 62, no. 7, pp. 70212, 2019.
[20] J. Zhao, H. Duan, L. Chen and M. Huo, "Leadership hierarchy-based formation control via adaptive chaotic pigeon-inspired optimization," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 9348–9353, 2020.
[21] G. N. Nguyen, N. H. Le Viet, A. F. S. Devaraj, R. Gobi and K. Shankar, "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 28, pp. 100464, 2020.