Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.025461
Article

Tech Science Press

Blockchain Enabled Metaheuristic Cluster Based Routing Model for Wireless Networks

R.M. Bhavadharini[1,*] and S. Karthik[2]

[1]Department of Computer Science and Engineering, Easwari Engineering College, Chennai, 600089, India
[2]Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, 641035, India
*Corresponding Author: R. M. Bhavadharini. Email: rmbhavadharini@gmail.com
Received: 24 November 2021; Accepted: 10 January 2022

Abstract: With recent advancements made in wireless communication techniques, wireless sensors have become an essential component in both data collection as well as tracking applications. Wireless Sensor Network (WSN) is an integral part of Internet of Things (IoT) and it encounters different kinds of security issues. Blockchain is designed as a game changer for highly secure and effective digital society. So, the current research paper focuses on the design of Metaheuristic-based Clustering with Routing Protocol for Blockchain-enabled WSN abbreviated as MCRP-BWSN. The proposed MCRP-BWSN technique aims at deriving a shared memory scheme using blockchain technology and determine the optimal paths to reach the destination in clustered WSN. In MCRP-BWSN technique, Chimp Optimization Algorithm (COA)-based clustering technique is designed to elect a proper set of Cluster Heads (CHs) and organize the selected clusters. In addition, Horse Optimization Algorithm (HOA)-based routing technique is also presented to optimally select the routes based on fitness function. Besides, HOA-based routing technique utilizes blockchain technology to avail the shared memory among nodes in the network. Sensor nodes are treated as coins whereas the ownership handles the sensor nodes and Base Station (BS). In order to validate the enhanced performance of the proposed MCRP-BWSN technique, a wide range of simulations was conducted and the results were examined under different measures. Based on the performance exhibited in simulation outcomes, the proposed MCRP-BWSN technique has been established as a promising candidate over other existing techniques.

Keywords: Wireless networks; blockchain; routing protocol; clustering; security; metaheuristics

1 Introduction

Recently, Wireless Sensor Network (WSN) has become a significant domain in the fields of communication, microelectronics, database, network, and so on. This is primarily because it is extensively applied in a wide range of domains. It integrates many technologies such as computing, sensing, and wireless transmission [1]. The physical target is monitored on a real-time basis via different

kinds of microsensors which in turn generate a huge amount of perceptive data at an unparalleled rate. Even though the application scenario and positioning of hardware are distinct, the fundamental objective remains the same i.e., to transmit, process, and collect the perceived data. At last, the users can obtain stimulating data from the information [2]. Being a data-centric network, WSN faces a significant challenge i.e., data storage of nodes which must be resolved. The user is more concerned about perspectives of data instead of the sensors or the networks that contain the sensors. Moreover, WSN assists reliable and efficient data storage from which access is possible under unreliable and heterogeneous environments. The research investigations conducted about efficient storage of data, overcoming the constrained storage space, form a significant area of research in WSN data management since energy and storage space of every node are constrained.

In hierarchical WSN, a sink node or otherwise a Cluster Head (CH), is widely employed in the aggregation of the sensed data from Cluster Members (CM). However, the clustered routing protocol is positioned for reducing energy consumption and network traffic [3,4]. Lower Energy Adaptive Clustering Hierarchy (LEACH) protocol is a traditional clustered routing protocol used for balancing the network load and reducing the power utilization [5]. In case of hierarchical WSN, when CHs are in high level and its data processing load gains too much of weight, the failure of high level CH might paralyze the entire networks. Simultaneously, when a CH, specifically a high level one, is compromised and captured, it breaches the data security of entire network.

Multi-hop routing technique is one of the significant technologies in WSN and is largely accountable for the transmission of data gathered by sensors from source to destination nodes based on the approved routing protocol [6]. But, the dynamic, open, and distributed features of WSN make the multihop routing, susceptible to different kinds of attacks. So, it severely impacts the effectiveness and security [7]. Conventional secure routing systems are targeted by certain selfish / malicious attacks. Therefore, it could not be applied in case of multihop-distributed WSN, since they are largely based on authentication mechanism encryption algorithm. In dynamic and time-varying WSN environments, current routing schemes could not precisely differentiate the malicious nodes. In certain routing algorithms, the routing node could not authenticate the routing data released by other routing nodes.

Data security issues mostly come from security attacks [8]. Generally, a security attack is classified as either internal or external attack intended towards WSN. Internal attacks include eavesdropping attacks, decoding attacks and probabilistic jamming attacks. External attacks are targeted at compromised nodes and its attack behavior includes discarding, tampering, forging, selective forwarding, and replaying of the data packets. It is possible to prevent the external attacks by authentication, encryption-based digital watermarking and other conventional security systems. On the contrary, this security system cannot give protection against internal attacks. This is because of the fact that compromised nodes contain keys and security algorithms [9]. Moreover, in case of resource-limited sensors, it is not possible to run the security algorithm which has higher computation complexity. In hierarchical WSN, the data security is now heavily increased in order to ensure the communication of sensed data which is secured with the help of lightweight authentication / encryption systems. But, due to the unattended placement of sensors, no efficient systems are in place for the prevention of compromise and capture of nodes. Thus, the internal attacks are made at these compromised nodes which could not be avoided as well. Concurrently, when a malicious node is selected as a CH, there is no assurance provided for both integrity and authenticity of the sensed data in whole cluster. Fortunately, various researches have displayed that trust management system is an efficient method to defend the internal attacks [10]. Furthermore, the trust values are adopted from these trust management systems as significant factors using which a secure CH is selected and a secure routing protocol is developed.

The current research paper focuses on the design of Metaheuristic-based Clustering with Routing Protocol for Blockchain-enabled WSN abbreviated as MCRP-BWSN. The proposed MCRP-BWSN

technique intends to utilize blockchain technology for shared memory schemes and optimal route selection in clustered WSN. MCRP-BWSN technique involves two major processes namely Chimp Optimization Algorithm (COA)-based clustering technique and Horse Optimization Algorithm (HOA)-based routing technique. Besides, HOA-based routing technique utilizes blockchain technology to avail shared memory among the nodes present in the network. In order to authenticate the superiority of the proposed MCRP-BWSN technique, a comprehensive experimental analysis was carried out and the results were assessed under distinct metrics.

The rest of the paper is organized as follows. Section 2 offers the literature review, Section 3 provides the proposed model, and Section 4 concludes the work.

2 Literature Review

The current section offers a detailed review on existing cluster-based routing techniques for blockchain-enabled WSN. Yang et al. [11] proposed a trusted routing system with blockchain and RL algorithm to improve the routing efficiency and security in WSN. A set of possible routing systems are provided to obtain the routing data of routing nodes on the blockchain in order to make the former impossible and non-traceable to tamper with. Reinforcement learning (RL) method is applied to help the routing nodes vigorously by the selection of efficient and trusted routing connections. Sahay et al. [12] proposed a layered IoT routing security method to analyze the susceptibilities with regards to every stage of the routing method. The authors examined the way to leverage the inherent characteristics of blockchain so as to enhance the routing security in IoT-Lossy Network Architecture (LLN). Then, a blockchain-based architecture was proposed using an intelligent contract to generate real-time alerts that can effectively find the sensors including the tampering of LLN configurational data.

Shahbazi et al. [13] proposed a blockchain-based Adaptive Thermal-/Energy-Aware Routing (ATEAR) protocol for WBAN. Power utilization, throughput, and temperature increase were used as calculation metrics to analyze the efficiency of ATEAR in data transmission. On the other hand, resource utilization, transaction throughput, and latency were applied in the investigation of blockchain scheme outcomes. Hyperledger Caliper, a benchmark tool, was utilized to assess the efficacy of blockchain method based on memory, and central processing unit (CPU) consumption. Nguyen et al. [14] introduced a novel energy-effective and secure clustering-based data transmission method from pervasive WSN, with RDA-based clustering method using blockchain-assisted secured data transmission abbreviated as red deer algorithm based clustering with blockchain (RDAC-BC). The clustering techniques perform CH election whereas the cluster construction method is developed. If a CH is selected, blockchain-assisted secure data transmission occurs between CHs and CMs.

Honar Pajooh et al. [15] proposed a multilayer blockchain security method for the protection of IoT networks, when simplifying the execution. In this study, clustering idea was used to facilitate the multilayer framework. K-unknown cluster was determined within the IoT network using the method that exploits a hybrid Evolutionary Computation Algorithm, a result of combining simulated annealing (SA) and genetic algorithm (GA). The selected CH is accounted for local authorization and authentication. The execution of local private blockchain facilitates the transmission between CHs and significant BSs. Dhurandher et al. [16] explored a decentralized and secure method in which a Proof of Work (PoW) consensus method was exploited to propose a BDRP approach. In this study, the authors designed and incorporated a routing protocol that utilizes PoW for routing process. The model was demonstrated for its immutability in OppNet model. Blockchain promises distributed, transparent, and secure systems and tamper-resistant ledger which altogether offer secure routing solutions for OppNet model.

In Awan et al. [17], a blockchain-based verification method was presented in which the identity of all nodes is saved in the blockchain. Both private and public blockchains were employed for verification. SN

was authenticated by private blockchain, whereas public blockchain authenticated the CHs. In the presented method, the trust values were evaluated for the removal of malicious node. A secure routing was executed based on the reliable nodes in the network. Wang et al. [18] proposed a light-weight blockchain-based secure routing method for swarm UAS networking. The study leveraged a light-weight blockchain method to enhance a secure routing for swarm UAS networking i.e., based on 5G NR cellular networking. Unlike traditional routing algorithm, the presented approach used light-weight blockchain which can prevent the malicious connection from attackers, identify the malicious UAS and alleviate it from malicious UAS.

Kudva et al. [19] proposed two stage detection systems in which during initial phase, the adjacent node calculates the trust separately. Next, a consortium blockchain-based scheme, using authorized RSU as validator, aggregates the trust scores for vehicular nodes. Later, based on the trust scores secured by the adjacent node, the blacklist nodes present in the table get changed vigorously. Ramezan et al. [20] proposed a novel BCR protocol for a network of untrusted IoT devices. Unlike traditional secure routing protocols, where a CA is required to facilitate the authentication and identification of all the devices, BCR protocols operate in a dispersed way without CA. BCR protocols utilize smart contracts to find a path for data gateway or destination within heterogeneous IoT network. Some intermediate devices could ensure a route from source IoT device to a gateway/destination device.

3 The Proposed Model

In current study, a new MCRP-BWSN technique is proposed to accomplish optimal route selection and security in the clustered WSN. The proposed MCRP-BWSN technique primarily makes use of COA-based clustering technique to choose the CHs from the available set of nodes. Then, HOA-based routing technique is employed to derive an optimal set of routes to BS. At the same time, HOA-based routing technique utilizes blockchain technology to avail the shared memory among nodes in the network. At the time of route selection, the transactions are saved in the blockchain with an intention to share the status of network in real-time environment. Fig. 1 demonstrates the overall working process of MCRP-BWSN model. The details of the processes involved in these tasks are discussed in the following sections.

3.1 Design of COA-Based Clustering Technique

During initial stage, the nodes are randomly placed in the network. Then, COA technique is applied in the selection of CHs and the clusters are constructed. COA is a new SI algorithm developed by Khishe and Mosavi in 2020 [21]. Its instinctive backgrounds originate from the hunting behaviors of chimps. Chimp performs a variety of activities based on the separation of labour to identification of the prey. In normal COA approach, the chimp group is divided into four types such as barrier, attacker, driver, and chaser. Amongst the four types, 'attackers' lead the population. The other three kinds of chimps support in hunting and accordingly, the status gets reduced in a consecutive manner. The arithmetical method is briefly determined as given herewith. Eqs. (1) & (2) are employed to update the location of the chimps.

$$\begin{aligned} X_1(t+1) &= X_{Attacker}(t) - a_1 \cdot d_{Attacker} \\ X_2(t+1) &= X_{\text{Barrier}}(t) - a_2 \cdot d_{\text{Barrier}} \\ X_3(t+1) &= X_{Chaser}(t) - a_3 \cdot d_{Chaser} \\ X_4(t+1) &= X_{Driver}(t) - a_4 \cdot d_{Driver} \end{aligned} \tag{1}$$

$$X_{chimp}(t+1) = \frac{X_1 + X_2 + X_3 + X_4}{4} \tag{2}$$

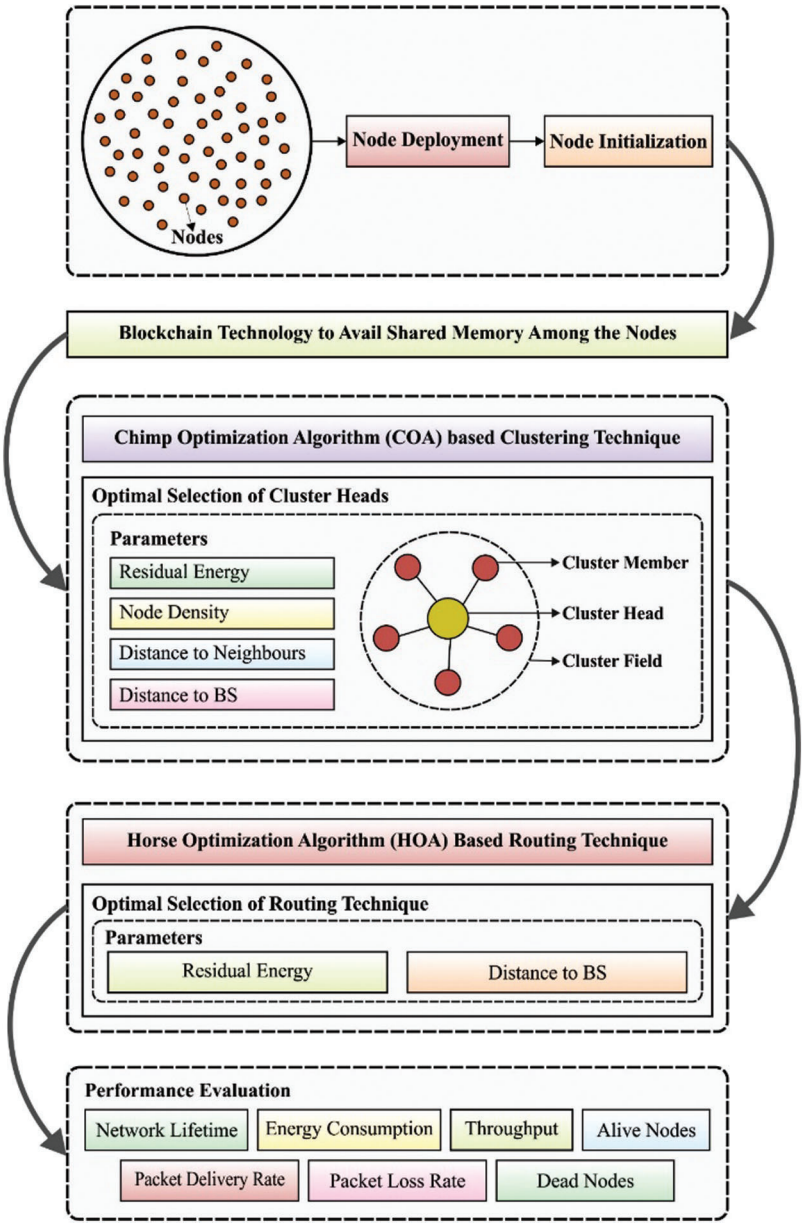

Figure 1: Overall process of MCRP-BWSN model

Whereas t represents the number of present iterations, the location of the chimps are upgraded based on four kinds of location considered i.e., X_{Barrier}, X_{Attacker}, X_{Driver} and X_{Chaser}. Vector d and dynamic coefficient a are shown in Eq. (3).

$$\begin{aligned} a_1 &= 2 \cdot f_1 \cdot r_1 - f_1, \; d_{Attacker} = |X_{\text{Attacker}}(t) - m \cdot X(t)| \\ a_2 &= 2 \cdot f_2 \cdot r_1 - f_2, \; d_{Barrier} = |X_{\text{Barrier}}(t) - m \cdot X(t)| \\ a_3 &= 2 \cdot f_3 \cdot r_1 - f_3, \; d_{Chaser} = |X_{\text{Chaser}}(t) - m \cdot X(t)| \\ a_4 &= 2 \cdot f_4 \cdot r_1 - f_4, \; d_{Driver} = |X_{\text{Driver}}(t) - m \cdot X(t)| \end{aligned} \tag{3}$$

Here, the coefficient f gets non-linearly minimizes from 2.5 to 0 with a lapse of iteration. $c = 2r_2 \cdot r_1$ and r_2 denote arbitrary values in the range of zero and one [22]. m indicates a chaotic map vector. Assume, in all likelihood that μ represents an arbitrary value in the range of zero and one and chaotic models are applied to the location upgrading while $\mu \geq 0.5$, as expressed in Eq. (4). Or else, Eq. (2) is yet to be performed. Algorithm 1 displays the pseudocode of COA method.

$$X_{\text{chimp}}(t+1) = \text{Chaotic\_}value \tag{4}$$

Algorithm 1: Pseudo-code of COA

Initiate the population size and the maximal amount of iterations

Initialize locations of chimp

Evaluate the fitness of all chimps

Chosse barrier, attacker, driver, and chaser.

When t< the maximal amount of iterations

For all the chimps

If $\mu < 0.5$

Upgrade the location of the present chimp by Eq. (2)

Else if

Upgrade the location of the present chimp by Eq. (4)

End if

End for

Update $X_{Barrier}$, $X_{Attacker}$, $X_{Driver,}$ and X_{Chaser}

t = t + 1

End while

Return $X_{Attacker}$

COA-based clustering method is derived at, in the presence of four fitness parameters namely, residual energy, node density, distance to neighbors, and distance from CH to BS. The fitness parameters are given herewith.

Residual energy: CHs carry out various procedures namely, sensing, collecting, aggregation and data broadcast. Therefore, CHs utilize the maximum energy than another node. After that, it is important to determine the Fitness Function (FF) which shares the load amongst all other sensors in the network. The fitness parameters for effectual usage of network energy are given herewith.

$$R_e = e(n_i)$$

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

$$f_1 = CH_{opt} * \frac{R_e}{Avg_e} = \frac{CH_{opt} * e(n_i)}{\frac{1}{n}\Sigma_{i=0}^{n} e(n_i)} \forall CH_{opt} = 5\% \; of \; n, \; e(n_i)$$

$$= 0.5J \; or \; 1.25J \; or \; 1.75J \tag{5}$$

where, R_e, Avg_e, and n_i denote node residual energy, network average energy and the total amount of SNs from the network. CH_{opt} refers to optimal percentage of CH. The objective function f_1 showcases the ratio of every node residual energy and network average energy.

Node density: During intra cluster communication, cost is a vital parameter to improve the energy performance of the network. The maximum node degree of the CHs results in effective network efficiency and it can be determined as follows.

$$f_2 = \max\left(n(CH_1), n(CH_2), n(CH_3) n\left(CH_j\right)\right) \forall n = 2\ To\ 95,\ j = 1\ to\ 15 \tag{6}$$

where $n\left(CH_j\right)$ implies the number of sensors in the range of j^{th} CH $\left(CH_j\right)$. The value of objective function f_2 is higher for right choice of CHs and it is utilized based on reducing energy consumption.

Distance to neighbors: In intracluster communication, the sensor transmits the data to CHs. If the CHs are reserved in a CM, then the sensors reduce the energy if CH is closer to the member where the nearby SNs employ minimal energy.

$$f_3 = \frac{1}{n_{s\tau}} \sum_{i=0}^{n_{sr}} disT(CH,\ i)\ \forall dist(CH,\ i) = 1\ to\ 35\ m, n_{sr} = 1\ to\ 100 \tag{7}$$

where, n_{sr} and $dist(CH,\ i)$ denote the number of sensors from sensing sequences and Euclidean distance between the nodes and CH.

Distance from CH to BS: For effective CH selection, the distance between CHs and BS becomes an essential function. This occurs particularly in case if the selected CH is distant from the BS and it utilizes the energy rapidly. This scenario is estimated from the functions given below.

$$f_4 = \frac{1}{CH} \sum_{\mathrm{i}=0}^{\mathrm{CH}} dist(BS,\ CH_i)\ \forall dist(BS,\ CH_i) = 1\ to\ 70m,\ CH = 1\ to\ 15 \tag{8}$$

where, $dist(BS,\ CH_i)$ signifies the Euclidean distance between BS and the i^{th} CH (CH_i). The f_4 objective function statement should be minimized so that the selected CHs are not distant to BS.

Once f_1, f_2, f_3, and f_4 function parameters are estimated, the objective function named FF is defined as follows.

$$F = Maximize\ Fitness\ = \alpha * f_1 + \beta * f_2 + \gamma * \frac{1}{f_3} + \delta * \frac{1}{f_4} \tag{9}$$

where, α, β, γ, and δ are the weighted coefficients for f_1, f_2, f_3, and f_4 FF parameters, correspondingly. The range of the weighted coefficient varies in the interval of [0,1].

3.2 HOA-Based Routing Technique Design

After CH selection and cluster construction processes, HOA is executed to perform the route selection process. The main inspiration of HOA is the hierarchical organization of horse herds. Horses prefer to live as herds. Since several animals live together as large groups, it is important and significant to determine a stable hierarchical scheme or 'pecking order' in order to increase group cohesion and mitigate aggression. It is often, but not always, a linear method. In nonlinear hierarchy, horse A might be superior to horse B, which in turn is superior to horse C. However, horse C might be superior to horse A. Superiority is decided based on several aspects and involves an individual's requirement for a certain resource at a certain moment. Therefore, it remains a variable all over the lifespan of herds or single animal. Few horses might be superior throughout the resource whereas others might be submissive for each resource. It must be noted that this is not a part of natural horse behaviour. It may at times be enforced by human being upon horses to live together in constraint space and less number of resources. Sometimes, a

dysfunctional social ability horse is also termed as 'superior horse'. Once the horses form a herd, their behaviour becomes hierarchical i.e., high ranking animal in the herd drinks and eat early. Herd members at low status eat at later stages while at times, some may not also get sufficient food. In case of low feed availability, high-ranked horses might have prevented the low-ranked ones from eating at all.

Horse herds have a superior mare/stallion and the hierarchical order of horse in a herd defines the priority of access to the resources. The hierarchy of a horse in a herd is calculated by the primary stage of the approach, considering its fitness value in that herd. Let us assume a herd of k horses and P denotes a function

$$Herd = \{H_1, \ldots, H_k\} \tag{10}$$

$$P = Herd \rightarrow \{1, \ldots, K\} \tag{11}$$

If fitness (H_x)<fitness $\left(H_y\right)$ where $x \neq y$ and x, $y\epsilon\{1 \ldots K\}$ then

$$P(H_x) > P\left(H_y\right) \tag{12}$$

If fitness (H_x)=fitness $\left(H_y\right)$ where $x \neq y$ and x, $y\epsilon\{1 \ldots K\}$ then

$$\left[P(H_x) - P\left(H_y\right)\right](x - y) > 0 \tag{13}$$

The rank of each horse H_x is determined as follows.

$$H_x - Rank\ of\ each\ horse = \frac{P(H_x)}{K} \tag{14}$$

All the herds have a centre one which is equivalent to the weighted average of the position of horse from herd. Thus, the weight is represented as the rank of horse [23]. The centre of the herds is computed as given herewith.

$$Herd_{Center} = \frac{\sum_{x=1}^{k} Z_x H_{x.rank}}{\sum_{x=1}^{k} H_{x.rank}} \tag{15}$$

The distance between the location of stallion and the center of horse herd 'H' is calculated by Euclidean distance as given herewith.

$$Dim(Stallion,\ herd) = \sqrt{\sum_{y=1}^{Dim} \left(Staalion_y - Herd_{Center}\right)^2} \tag{16}$$

Here, *Dim* denotes the number of dimensions in search space. When the horse belongs to a herd of horses, it upgrades its velocity as follows.

$$Vel_{x,y}^{T+1} = Vel_{x,y}^{T} + H_{x.rank} * \left(Herd_{center.y}^{T} - Z_{x,y}^{t}\right) \tag{17}$$

$$Vel_{x,y}^{T+1} = Vel_{x,y}^{T} + Rand * \left(Herd_{center.y}^{T} - Z_{x,y}^{t}\right) \tag{18}$$

where *Rand* is a random number from [0,1]. T denotes the present iteration and $T + 1$ indicates the novel iteration. The memory of horse (Mem) is a matrix containing a quantity of rows equivalent to the values of HMP of D column and horse.

$$Mem_x^{T+1} = \begin{bmatrix} Mem_{1,x,1}^{T+1} & \cdots & Mem_{1,x,D}^{T+1} \\ \vdots & \ddots & \vdots \\ Mem_{HMP,x,1}^{T+1} & \cdots & Mem_{HMP,x,1}^{T+1} \end{bmatrix} \tag{19}$$

The equation employed to update the cells of memory matrix is as follows.

$$Mem_{K,x,y}^{T+1} = Z_{x,y}^{T+1} * N(0, SD) \tag{20}$$

where N represents a standard distribution with mean zero and standard deviation (SD). HOA derives a fitness value of every solution or route between the CHs and BS. The aim of HOA-based routing technique is to determine the route utilizing less energy and at less distance. Fitness function can be considered as a minimization function and is represented as follows.

$$F_i = \min \{\mathrm{RE}_i \times DIST_i\} \tag{21}$$

where, 'F_i' denotes the fitness of ith population, 'RE_i' is the energy needed for ith population and '$DIST_i$' refers to the total distance of ith route or population. In HOA, the existing routes between CH and BS are initialized as primary populations. At the beginning, CH becomes a transmission whereas other CHs or BS gets transformed into a destination. Therefore, the probable routes from CH to BS are defined as follows.

$$Sol = P_i, \quad i = 1, 2, \ \cdots, N. \tag{22}$$

where 'Sol' signifies the initial population set, 'P_i' designates the ith route from CH to BS, and 'N' denotes the count of routes. The route comprises of distance and total energy as given below.

$$P = \{RE, \ DIST\} \tag{23}$$

where 'RE' denotes the remaining energy of node in the route whereas 'DIST' denotes the total distance of the route. The standard deviation for RE (σ_{RE}) is employed in the determination of value of uniform load dispersal amongst sensors, as defined below.

$$RE = f_1 = \sigma_{RE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n} \left\{\mu_{RE} - e\left(node_j\right)\right\}^2} \tag{24}$$

$$\mu_{RE} = \frac{1}{n}\sum_{i=1}^{n} E(node_i)$$

Followed by, the distance from CH to BS can be determined by total Euclidean distance between every CH in the route, as represented in (25).

$$DIST = \sum_{i}^{n-1} \sqrt{(CH_i(x) - CH_{i+1}(x)) + (CH_i(y) - CH_{i+1}(y))} \tag{25}$$

where, '$CH_i(x)$' and '$CH_i(y)$' denote x and y coordinates of ith CH in the route correspondingly.

3.3 Blockchain Design as a Shared Memory Scheme

Blockchain is a group of blocks in which every block has four sections such as hash value of the prior block, data about the transactions (ethereum, bitcoin), timestamp, and current block. Blockchain is determined as a distributed electronic ledger and it can be employed in saving the transaction data through different points. The transaction can be recorded by a cryptographic hash value and confirmed by

each miner. It may possess the same values in comprehensive ledger and is made up of blocks of each transaction. Blockchain provides the capacity to share ledger details in a protected way. Decentralized storage is a basic characteristic in blockchain whereas maximal data could be transferred and recorded from current block to prior block through a smart contract code. In LitecoinDB, Swarm, SiacoinDB, MoneroDB, BigchainDB, and Interplanetary File System (IPFS), distinct features are employed in the decentralized database. Fig. 2 illustrates the framework of blockchain.

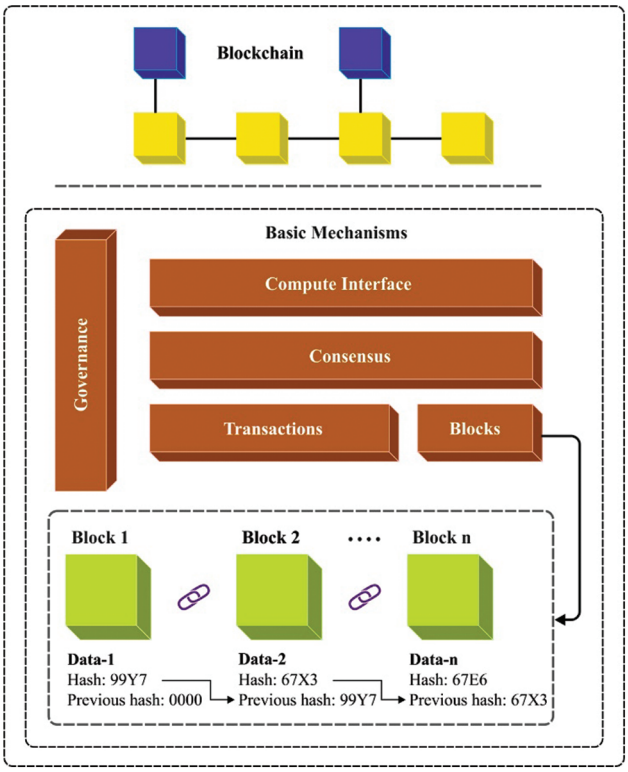

Figure 2: Framework of blockchain

Blockchain system depends on a ledger that keeps track of every transaction which is circulating in a network. Therefore, a certain way is required to determine the nodes that are being transferred and through which path they get transferred. This way, one can save the paths in real time, active, transactions in the blockchain. In order to achieve this, the network nodes are processed as coins. To be specific, certain nodes transfer a message from one source to BS and its ownership get influenced by the source node. Initially, each node possesses a BS and all the nodes possess BS which are deliberated as inactive [24]. In other terms, each node does not possess an active BS. Then, it asks the BS to transfer the path node ownership to it. When the transactions are registered with blockchain, the nodes get transferred via the selected route. Once the data is transferred effectively, to the BS, the transferring nodes transmit back the ownership of the path node, to BS including itself. This is only to ensure that the networks are notified about the peer, where the communication was completed. After this, such nodes are discharged. They consider that a source node is capable of owning u nodes when $u \leq n$.

Further, it is also considered that the node transmits on two channels. Initially, it is dedicated to path claiming and the transmission of blockchain transaction only. Later on, it is developed to carry forward sensitive information too. Primarily, they are attracted to succeeding channels that can be employed in the

transmittance of the message. Also, assume that all the intermediate nodes can be possessed, merely, through a single source node whereas a source node can be possessed, merely by itself. Once a node senses an activity, when it is possessed by another node, the last one waits for action, till its ownership is transferred to the BS. Meanwhile, the node informs the BS, through primary channel, to add in the waiting queue. Most of the waiting queues are dealt with BS. So, it is essential to prioritize the waiting node. As already mentioned, this approach enables a good knowledge about the source node and the path that they transfer over, at a certain point of time. The change in these numbers denote the number of messages transferred through a node, because a node status gets altered merely, while it is in the path where the messages are transferred

4 Performance Validation

The current section investigates the performance of the proposed MCRP-BWSN technique under different aspects. Tab. 1 provides the results of a detailed comparison of MCRP-BWSN technique against existing techniques in terms of PDR, throughput, and PLR.

Table 1: Results of the analysis of MCRP-BWSN model under different measures

Packet Delivery Ratio (PDR)						
No. of Nodes	PSO-CA	GA-CA	ALO-CA	GWO-CA	RDAC-BC	MCRP-WSN
100	0.941	0.947	0.958	0.968	0.993	0.998
200	0.932	0.940	0.952	0.963	0.989	0.993
300	0.925	0.936	0.945	0.958	0.980	0.982
400	0.917	0.928	0.939	0.951	0.975	0.987
500	0.910	0.922	0.931	0.943	0.968	0.979
Throughput (Mbps)						
No. of Nodes	PSO-CA	GA-CA	ALO-CA	GWO-CA	RDAC-BC	MCRP-WSN
100	70.05	83.05	87.85	89.95	98.00	99.56
200	63.99	76.10	81.90	83.91	95.00	98.75
300	61.00	67.95	75.00	76.99	91.00	97.89
400	56.05	61.00	68.09	72.00	88.00	92.35
500	51.00	55.09	60.89	69.05	86.00	89.86
Packet Loss Rate						
No. of Nodes	PSO-CA	GA-CA	ALO-CA	GWO-CA	RDAC-BC	MCRP-WSN
100	0.059	0.053	0.042	0.032	0.007	0.002
200	0.068	0.060	0.048	0.037	0.011	0.007
300	0.075	0.064	0.055	0.042	0.020	0.018
400	0.083	0.072	0.061	0.049	0.025	0.013
500	0.090	0.078	0.069	0.057	0.032	0.021

Fig. 3 depicts the results of achieved by MCRP-BWSN technique in terms of PDR under varying node counts. The results demonstrate that the proposed MCRP-BWSN technique accomplished effectual outcomes with maximum PDR. For instance, under 100 nodes, a high PDR of 0.998 was obtained by MCRP-BWSN technique, whereas particle swarm optimization (PSO)-CA, genetic algorithm (GA)-CA, ant lion optimizer (ALO)-CA, grey wolf optimization (GWO)-CA, and RDAC-BC techniques attained the least PDR values such as 0.941, 0.947, 0.958, 0.968, and 0.993 respectively. Simultaneously, under 300 nodes, an increased PDR of 0.982 was obtained by MCRP-BWSN technique, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques achieved low PDR values such as 0.925, 0.936, 0.945, 0.958, and 0.980 correspondingly. Concurrently, at 500 nodes, a maximum PDR of 0.979 was accomplished by the proposed MCRP-BWSN technique, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques accomplished minimum PDR values such as 0.910, 0.922, 0.931, 0.943, and 0.968 correspondingly.

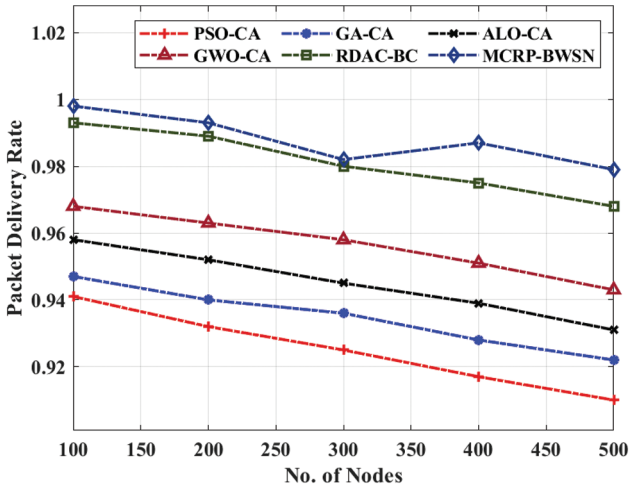

Figure 3: PDR analysis of MCRP-BWSN model

Fig. 4 showcases the results of the analysis of MCRP-BWSN approach with respect to throughput under different node counts. The results showcase that the proposed MCRP-BWSN model accomplished effective outcomes with maximum throughput. For instance, at 100 nodes, a maximum throughput of 99.56 Mbps was achieved by MCRP-BWSN method, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC algorithms gained lesser throughput values such as 70.05 Mbps, 83.05 Mbps, 87.85 Mbps, 89.95 Mbps, and 98 Mbps correspondingly. Concurrently, under 300 nodes, an enhanced throughput of 97.89 Mbps was achieved by the proposed MCRP-BWSN method, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC methodologies gained low throughput values such as 61 Mbps, 67.95 Mbps, 75 Mbps, 76.99 Mbps, and 91 Mbps respectively. Similarly, at 500 nodes, a high throughput of 89.86Mbps was obtained by the proposed MCRP-BWSN method, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC methodologies achieved low throughput values such as 51 Mbps, 55.09 Mbps, 60.89 Mbps, 69.05Mbps, and 86Mbps correspondingly.

A detailed PLR analysis was conducted upon MCRP-BWSN technique under different node counts and the results are displayed in Fig. 5. The figure reports that the proposed MCRP-BWSN technique gained superior performance with minimum PLR. For instance, at 100 nodes, a minimum PLR of 0.002 was accomplished by MCRP-BWSN technique, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques achieved high PLR values such as 0.059, 0.053, 0.042, 0.032, and 0.007 respectively. Moreover, under 300 nodes, a minimum PLR of 0.018 was attained by MCRP-BWSN

method, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC algorithms produced superior PLR values such as 0.075, 0.064, 0.055, 0.042, and 0.020 correspondingly. Furthermore, at 500 nodes, a minimum PLR of 0.021 was achieved by MCRP-BWSN technique, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC algorithms accomplished maximum PLR values such as 0.090, 0.078, 0.069, 0.057, and 0.032 correspondingly.

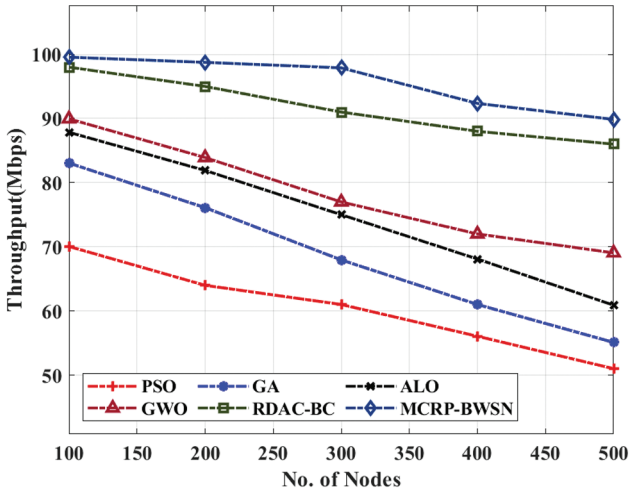

Figure 4: Throughput analysis of MCRP-BWSN model

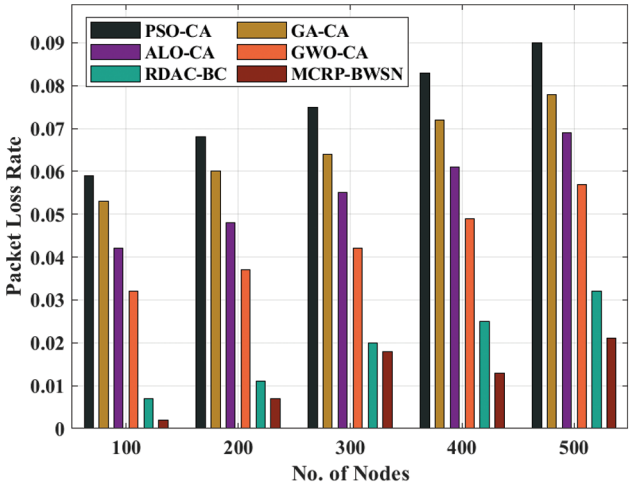

Figure 5: PLR analysis of MCRP-BWSN approach

Tab. 2 shows the results of a detailed comparison analysis of MCRP-BWSN method against existing techniques with respect to EC and NLT. A brief EC analysis was conducted upon MCRP-BWSN method under different node counts and the results are displayed in Fig. 6. The figure reports that MCRP-BWSN technique produced superior performance with minimal EC value. For instance, at 100 nodes, a low EC of 0.046 mJ was achieved by MCRP-BWSN technique, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques produced increased EC values such as 0.201 mJ, 0.172 mJ, 0.136 mJ, 0.120 mJ, and 0.080mJ correspondingly. Besides, under 300 nodes, a low EC value 0.208mJ was yielded

by the proposed MCRP-BWSN method, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC approaches produced high EC values such as 0.552 mJ, 0.564 mJ, 0.482 mJ, 0.462 mJ, and 0.230 mJ respectively. Additionally, at 500 nodes, a minimum EC of 0.332mJ was obtained by the proposed MCRP-BWSN technique, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC models yielded high EC values such as 0.883 mJ, 0.823 mJ, 0.702 mJ, 0.731 mJ, and 0.410 mJ correspondingly.

Table 2: Results of the analysis of MCRP-BWSN model against existing techniques

Energy Consumption (mJ)						
No. of Nodes	PSO-CA	GA-CA	ALO-CA	GWO-CA	RDAC-BC	MCRP-BWSN
100	0.201	0.172	0.136	0.120	0.080	0.046
200	0.420	0.334	0.259	0.274	0.150	0.115
300	0.552	0.564	0.482	0.462	0.230	0.208
400	0.720	0.663	0.607	0.598	0.350	0.277
500	0.883	0.823	0.702	0.731	0.410	0.332
Network Lifetime (Rounds)						
No. of Nodes	PSO-CA	GA-CA	ALO-CA	GWO-CA	RDAC-BC	MCRP-BWSN
100	1350	1455	1510	1535	1600	1875
200	1665	1763	1845	1885	2020	2437
300	2250	2225	2348	2375	2580	2762
400	2673	2770	2818	2850	3152	3356
500	3078	3280	3273	3420	3499	3980

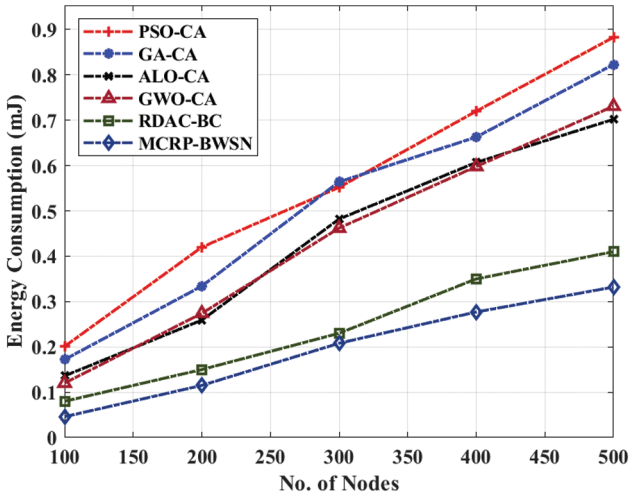

Figure 6: EC analysis of MCRP-BWSN model with distinct nodes

Fig. 7 illustrates the results from the analysis of MCRP-BWSN model in terms of NLT under distinct node counts. The outcomes portray that the proposed MCRP-BWSN method accomplished effective outcomes with maximum NLT. For sample, at 100 nodes, an improved NLT of 1875 rounds was reached

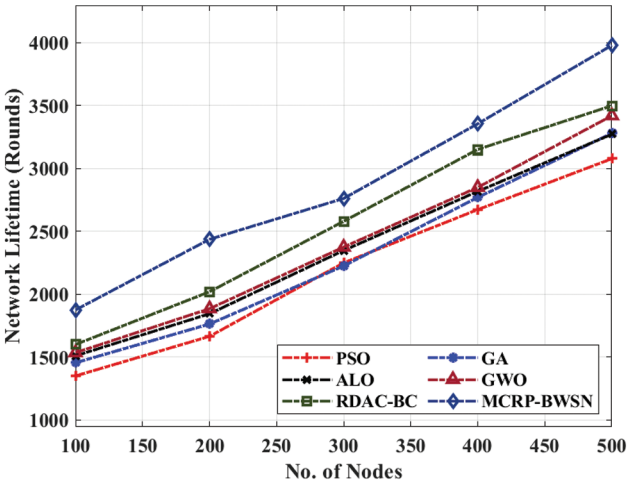

Figure 7: NLT analysis of MCRP-BWSN model with different nodes

by the proposed MCRP-BWSN methodology, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques attained the least NLT values such as 1350, 1455, 1510, 1535, and 1600 rounds correspondingly. At the same time, with 300 nodes, a maximum NLT of 2762 rounds was achieved by MCRP-BWSN technique whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques accomplished the least NLT values such as 2250, 2225, 2348, 2375, and 2580 rounds respectively. Concurrently, with 500 nodes, a maximum NLT of 3980 rounds was attained by the proposed MCRP-BWSN model, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques provided minimal NLT values such as 3078, 3280, 3273, 3420, and 3499 rounds correspondingly.

A comprehensive NDN analysis was conducted upon MCRP-BWSN method under different node counts and the results are displayed in Tab. 3 and Fig. 8. The figure states that the proposed MCRP-BWSN model achieved maximum performance with the least NDN. For instance, under 1200 nodes, a low NDN of 10 was achieved by MCRP-BWSN method, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC methods resulted in high NDN values such as 149, 157, 94, 84, and 17 respectively. Likewise, at 2400 nodes, a low NDN of 30 was accomplished by MCRP-BWSN algorithm, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC techniques produced high NDN values such as of 309, 283, 227, 254, and 60 correspondingly. Besides, with 3500 nodes, a minimum NDN of 289 was attained by MCRP-BWSN method, whereas PSO-CA, GA-CA, ALO-CA, GWO-CA, and RDAC-BC approaches resulted in high NDN values such as 499, 499, 499, 499, and 370 correspondingly.

Table 3: NDN analysis of MCRP-BWSN model

No. of dead sensor nodes (NDN)						
No. of rounds	PSO-CA	GA-CA	ALO-CA	GWO-CA	RDAC-BC	MCRP-BWSN
400	109	99	55	29	0	0
800	129	113	75	59	8	3
1200	149	157	94	84	17	10
1600	190	161	115	94	25	15
2000	208	176	125	113	32	22

(Continued)

Table 3 (continued).

No. of dead sensor nodes (NDN)						
No. of rounds	PSO-CA	GA-CA	ALO-CA	GWO-CA	RDAC-BC	MCRP-BWSN
2400	309	283	227	254	60	30
2800	452	362	321	336	130	105
3200	499	477	473	468	212	176
3500	499	499	499	499	370	289

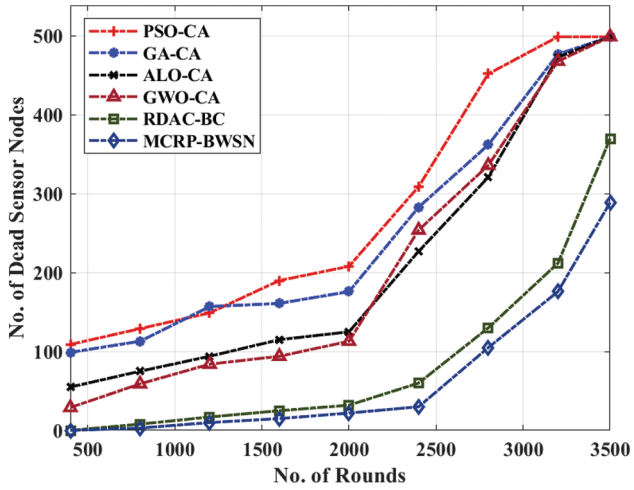

Figure 8: NDN analysis of MCRP-BWSN model with distinct rounds

5 Conclusion

In current study, a novel MCRP-BWSN technique was proposed to accomplish optimal route selection and security in WSN. The proposed MCRP-BWSN technique involves two major stages such as COA-based clustering process and HOA-based routing process. Besides, COA and HOA techniques derived a fitness function using different input parameters for effective CH and route selection. In addition, the transactions are saved in the blockchain with an intention to share the status of network in real-time environments. In order to authenticate the superiority of the proposed MCRP-BWSN technique, a comprehensive experimental analysis was carried out and the results were assessed under distinct metrics. The experimental results highlight that the proposed MCRP-BWSN technique produced significant outcomes over other existing techniques. As a part of future scope, MCRP-BWSN technique can be applied in mobile adhoc networks and vehicular networks.

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] J. Yick, B. Mukherjee and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] H. Cheng, Z. Xie, L. Wu, Z. Yu and R. Li, "Data prediction model in wireless sensor networks based on bidirectional LSTM," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 203, 2019.

[3] M. Satheesh Kumar, S. Vimal, N. Z. Jhanjhi, S. S. Dhanabalan and H. A. Alhumyani, "Blockchain based peer to peer communication in autonomous drone operation," *Energy Reports*, vol. 7, no. 2, pp. 7925–7939, 2021.

[4] S. P. Ahuja and N. Wheeler, "An introduction to using blockchain for internet of things security," *International Journal of Blockchains and Cryptocurrencies*, vol. 2, no. 1, pp. 1, 2021.

[5] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. of the 33rd Annual Hawaii Int. Conf. on System Sciences*, Maui, HI, USA, vol. 1, pp. 10, 2000.

[6] N. Kumar and Y. Singh, "Routing protocols in wireless sensor networks," in *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures*, Hershey, PA, USA: IGI Global, pp. 86–128, 2017.

[7] C. Xu, J. Ren, D. Zhang, Y. Zhang, Z. Qin *et al.,* "GANobfuscator: Mitigating information leakage under gan via differential privacy," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2358–2371, 2019.

[8] X. Wang, Z. Ning, M. C. Zhou, X. Hu, L. Wang *et al.,* "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1314–1345, 2019.

[9] W. Fang, W. Zhang, Y. Yang, Y. Liu and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution," *Science China Information Sciences*, vol. 60, no. 4, pp. 040305, 2017.

[10] W. Fang, C. Zhang, Z. Shi, Q. Zhao and L. Shan, "BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 59, no. 2, pp. 88–94, 2016.

[11] J. Yang, S. He, Y. Xu, L. Chen and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, pp. 970, 2019.

[12] R. Sahay, G. Geethakumari and B. Mitra, "A novel blockchain based framework to secure IoT-LLNs against routing attacks," *Computing*, vol. 102, no. 11, pp. 2445–2470, 2020.

[13] Z. Shahbazi and Y. C. Byun, "Towards a secure thermal-energy aware routing protocol in wireless body area network based on blockchain technology," *Sensors*, vol. 20, no. 12, pp. 3604, 2020.

[14] G. N. Nguyen, N. H. L. 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.

[15] H. H. Pajooh, M. Rashid, F. Alam and S. Demidenko, "Multi-layer blockchain-based security architecture for internet of things," *Sensors*, vol. 21, no. 3, pp. 772, 2021.

[16] S. K. Dhurandher, J. Singh, P. Nicopolitidis, R. Kumar and G. Gupta, "A blockchain-based secure routing protocol for opportunistic networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 4, pp. 3191, 2021.

[17] S. Awan, M. B. E. Sajid, S. Amjad, U. Aziz, U. Gurmani *et al.,* "Blockchain based authentication and trust evaluation mechanism for secure routing in wireless sensor networks," in *Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing*, Cham, Springer, pp. 96–107, 2021.

[18] J. Wang, Y. Liu, S. Niu and H. Song, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Computer Communications*, vol. 165, no. 7, pp. 131–140, 2021.

[19] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil *et al.,* "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing*, vol. 152, no. 9, pp. 144–156, 2021.

[20] G. Ramezan and C. Leung, "A blockchain-based contractual routing protocol for the internet of things using smart contracts," *Wireless Communications and Mobile Computing*, vol. 2018, no. 1, pp. 1–14, 2018.

[21] M. Khishe and M. R. Mosavi, "Chimp optimization algorithm," *Expert Systems with Applications*, vol. 149, no. 1, pp. 113338, 2020.

[22] H. Jia, K. Sun, W. Zhang and X. Leng, "An enhanced chimp optimization algorithm for continuous optimization domains," *Complex & Intelligent Systems*, vol. 15, no. 8, pp. 1542, 2021.

[23] D. Moldovan, "Horse optimization algorithm: A novel bio-inspired algorithm for solving global optimization problems," in *Computer Science On-line Conf.*, Cham, Springer, pp. 195–209, 2020.

[24] H. Lazrag, A. Chehri, R. Saadane and M. D. Rahmani, "A blockchain-based approach for optimal and secure routing in wireless sensor networks and IoT," in *2019 15th Int. Conf. on Signal-Image Technology & Internet-Based Systems (SITIS)*, Sorrento, Italy, pp. 411–415, 2019.