Computers, Materials & Continua
DOI:10.32604/cmc.2021.014180
Article

Tech Science Press

Energy-Efficient and Blockchain-Enabled Model for Internet of Things (IoT) in Smart Cities

Norah Saleh Alghamdi[1,*] and Mohammad Ayoub Khan[2]

[1]College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[2]College of Computing and Information Technologies, University of Bisha, Bisha, 67714, Saudi Arabia
*Corresponding Author: Norah Saleh Alghamdi. Email: nosalghamdi@pnu.edu.sa
Received: 04 September 2020; Accepted: 13 October 2020

Abstract: Wireless sensor networks (WSNs) and Internet of Things (IoT) have gained more popularity in recent years as an underlying infrastructure for connected devices and sensors in smart cities. The data generated from these sensors are used by smart cities to strengthen their infrastructure, utilities, and public services. WSNs are suitable for long periods of data acquisition in smart cities. To make the networks of smart cities more reliable for sensitive information, the blockchain mechanism has been proposed. The key issues and challenges of WSNs in smart cities is efficiently scheduling the resources; leading to extending the network lifetime of sensors. In this paper, a linear network coding (LNC) for WSNs with blockchain-enabled IoT devices has been proposed. The consumption of energy is reduced for each node by applying LNC. The efficiency and the reliability of the proposed model are evaluated and compared to those of the existing models. Results from the simulation demonstrate that the proposed model increases the efficiency in terms of the number of live nodes, packet delivery ratio, throughput, and the optimized residual energy compared to other current techniques.

Keywords: IoT; blockchain; WSN; smart cities; LNC

1 Introduction

Smart cities use the latest information and communication technology (ICT) to strengthen public infrastructure, utilities and public services. Smart cities can be viewed as an application of increasing population and urban development growth that has strengthened innovative ways of managing urbanization with minimal environmental impacts, civil lifestyles and governance [1]. Sensors are used in a large area across the city to track and control the smart city application. Typical examples include traffic systems, healthcare systems, toll collection systems, automatically identifying road data and automatically identifying vehicle number plates. Data centres and analytical engines are the backbone in smart cities for decision making process. In smart cities, the network of wireless devices, cameras, and sensors allows managing agencies to efficiently provide mandatory services and actions. Furthermore, smart cities use recycled materials for building facility centres and reducing energy usage; in order to make them more friendly environment. Fig. 1 shows the life cycle of smart cities consisting of four phases. The cycle

starts with the data collection from different sensors and connected devices. This first phase identifies and analyzes the data sources. The second phase of the life cycle is to clean, format and analyze the collected data. The third phase is about communications. This phase organizes the insights from analysis and communicates with decisions makers through use of strong networks. The fourth phase is for performing actions. It creates solutions from insights and optimizes solutions to improve the quality of life.

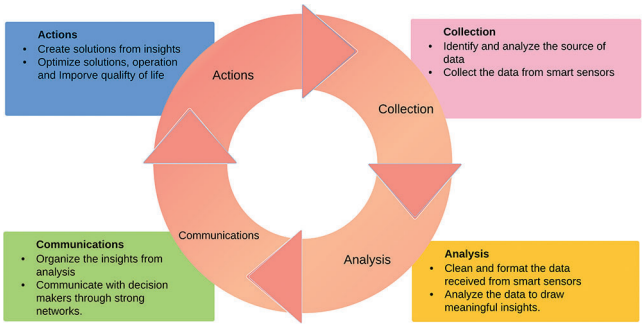

Figure 1: Life cycle of smart cities

Smart cities provide an effective and intelligent service delivery network for citizens and municipal corporation employees, through the installation of sensors to collect the information and to take appropriate actions [1,2]. WSNs bring IoT applications for better capabilities for both actuation and sensing. The WSN solutions cover a wide variety of applications, research, and advances in the technologies that have been continually expanding the field of applications. This trend in research leads to an upsurge in their uses of the applications of IoT networks for the low-cost versatile data actuation and sensing [3–7]. In IoT, all nodes transmit the sensor data straightforward to the internet. For example, a sensor can be deployed to record and to directly send the environmental parameters to a server either instantly or regularly using the internet. The server upon the received data will be processed and interpreted for further actions. The sensors are connected to a special kind of the sensor node, called cluster head (CH), to communicate with the servers [8,9]. WSNs are considered a system connected with IoT system using some cloud technologies. Every wireless sensor node comprises of computing, sensing devices, power components and radio transceivers. Typically, WSNs hold thousands of sensor nodes. Due to the demand for the low consumption of energy and the low complexity of devices, a consistent balance between the data processing abilities and the communications must be established [10,11]. Thus; the resource constraints and its heterogeneity in WSNs present new problems for the network management, particularly in smart cities, like the smart grids, the intelligent transportation systems and the smart buildings. The challenges in WSNs include the network life, the battery life, the *ad hoc* topologies, the sensor's maintenance and the resource allocation. To reduce the complexity in WSNs, an efficient clustering algorithm is required. The clustering is termed as the grouping of same type of objects [12]. A cluster of a group is defined as a segment of elements selected to reduce some dissimilarity [13]. Recent research has shown that the hierarchical routing algorithms have greater adaptability and low energy consumption compared to the flat routing algorithms for WSNs on a large scale [14,15].

In WSNs, the routing is a crucial part, where the sensors sense the data, and forwarding them to a sink node for processing. Nowadays, the sensors are available in cheap prices and in smaller sizes; however, there are still energy constraints. Generally, in all the routing algorithms, the data is traversed through multiple intermediate nodes before reaching to the sink node that consumes much of the energy. Therefore, there is a need to develop new algorithms which provide energy efficient routing.

This research study proposes K-means clustering algorithm for cluster head selection followed by a linear network coding for WSNs consisting of a blockchain enabled IoT devices. The contribution of this research study is to propose a WSN model with the blockchain based IoT devices; thereafter, forming K-means clustering of devices [12] to minimize the energy consumption in the intermediate nodes. Another contribution of this work is to implement LNC mechanism and to develop the blockchain to improve the security, and the reliability.

The remaining sections of this paper are arranged as follows: The related work and discussion are presented in Section 2; while the proposed methodology is presented in Section 3; The results and discussion are presented in Section 4; and Section 5 presents the conclusion and future work of the research.

2 Literature Review

Taheri et al. [16] suggested a clustering protocol coined with fuzzy logic that is primally based on a multi-hop. The proposed method of the clustering has three stages. The knowledge about the neighbor's is modified in the initial stage and the fuzzy output is measured. Every node sensor is remotely located at some points in the later phase until the delay time to listen to the CH message. If it fails, it announces itself to be a temporary CH and places the message simultaneously inside the boundary of the cluster. In the next iteration, it becomes the last CH and transmits a message if it has the least cost between the temporary cluster heads in the vicinity.

Gnanambigai et al. [17] surveyed the low energy adaptive clustering hierarchy (LEACH) and the variant protocols. They concluded that WSNs are in a need of more scalable and energy efficient algorithms. The drawback of the LEACH cluster head selection is that the CH selection occurs randomly [18–20]. Because of this particular criterion, there are chances that a low-energy sensor node may be selected as CH.

Suresh et al. [21] devised an energy-efficient dual CH selection method for WSNs. In this method, two cluster heads-specifically, the primary and secondary cluster heads - are picked with respect to parameters like the node degree, the residual energy, the least standard distance from the member nodes' timer using the particle swarm optimization procedure. When a supply node desires to broadcast information to the destination node, an energy-efficient direction-finding protocol is utilized, based on factors such as the anticipated number of the retransmissions and the possibility of a breakdown in a connection. In this method, every cluster node transmits the information to the primary CH node, then after, the collected information is broadcasted to base station (BS) via the secondary CH node.

Researchers have intensively modified the LEACH protocol to improve the efficiency of the network. The research community has been energetically contributing to improve the existing schemes and methodologies in order to improve the performance of the IoT networks [22]. For example, the energy-efficient method of trust derivation for WSN-based IoT networks has been explored in Duan et al. [23].

Sharma et al. [24] proposed a methodology to enhance the lifespan of the LEACH protocol using neural networks. They implemented an intelligent energy preservation model for the LEACH protocol called as LEACH-C algorithm which has increased lifespan. The nodes having the maximum energy of all are the best choice for CH.

Jamadar et al. [25] proposed an innovative energy-efficient WSNs using the K-means clustering algorithm. This method works on the basis of discovering the CH node with minimum distance from the centroid in terms of the Euclidean distance. The sensor is labelled as the CH node if the distance is lesser than the defined threshold value. K-means clustering protocol is employed in order to perform clustering of nodes which separates the sensor nodes to form K-clusters. Because of the successful CH nodes, the overall effectiveness of WSNs is improved with the respect to the parameters like the lively nodes and the spent energy for the transmissions.

Hwang and Huang [26] provided a secure channel of the communication in WSNs that are designated as a collector by a smart card owner to securely gather the data from the nodes which validates the collector and sending the data via a secure channel to the collector. By using the lightweight computing, the collector verifies the identification of the card's owner. This approach reduced the cost of communication.

Qin et al. [27] suggested the importance of the trust sensing algorithm for the routing that improves the security in WSNs. The aim of this mechanism used to control the attacks of the common networks affected by the inadequate energy and the defective deployment of the nodes on the networks for the data transactions in WSNs. Authors presented a trustworthy and secure routing scheme using attributes of a lightweight algorithm. The scheme provided resistance against several communication attacks at the same time.

Behera et al. [28] focused on the cluster head selection that interchanges the positions of the CH node among the cluster members having a maximum level of the energy. The algorithm takes into consideration, the residual energy, the initial energy, and the optimally selected CHs for selecting the succeeding set of CHs for WSNs.

Sun et al. [29] examined the effectiveness of the blockchain based network of IoT devices. In this work, authors proposed the spatio-temporal domain Poisson distribution. In this approach, the spatially distributed nodes and the rate data arrival were modelled as the Poisson point process (PPP). The successful blockchain transaction rate, throughput and the signal to interference noise ratio were derived.

3 Proposed Methodology

In the literature survey, we have observed that all the existing work to save the energy in the WSN-IoT systems are based on the parameters like the load balancing, the selection of cluster head, the minimum distance from centroid, the modified LEACH and the dual cluster head [16,17,21–29]. None of these works have addressed the energy saving using the coding technique. The proposed model is accompanied by the linear network coding to minimize the frequency of the direct transmissions with the BS. The security of the proposed energy-efficient model is coined using a blockchain. The blockchain provides decentralized availability of the information that is distributed through a network which is based on its participant's trust [30]. The architecture of the proposed WSN-IoT model is illustrated in Fig. 2 which shows the selection of an appropriate CH using K-means, the encoding using LNC and the security through the blockchain network. The architecture has four components: (i) The WSN-IoT network; (ii) Gateway; (iii) The Blockchain network and (iv) The IoT applications. The first component is the WSN-IoT network which is the collection of the WSN nodes and the IoT devices. The WSN nodes sense the information from the environment and performing the routing function. The WSN nodes are also responsible for the clustering whereas the IoT devices are responsible for the data encoding using LNC. The second component is Gateways, which is responsible for the data reception and forwarding to the blockchain network as illustrated in Fig. 2. The WSN network and Gateway are connected through the base station. The sensor's data are inserted into the blockchain network using the consensus mechanism. The application layer retrieves the data from the blockchain network and performing the data analytics to initiate the appropriate actions in the applications of the smart cities.

3.1 Network Model

Consider the situation where there are N uniformly distributed nodes in the $N \times N$ square area. The assumptions about the participating nodes, BS, the location, the communication model of the underlying network model are presented as follows:

1. In the typical sensor network application, the nodes and the base station are all immovable once the deployment is finished.

2. The transmission is secured using the blockchain network.
3. The sensors nodes are assumed to be heterogeneous with varying the initial energy.
4. The geographical information of the sensors is known in advance.
5. All the clusters are connected to a single BS that is reasonably away from the sensing field.
6. This simulation model considers the one-hop communication to reduce delay. In the proposed model, the CHs communicate directly with the sensor nodes or BSs.

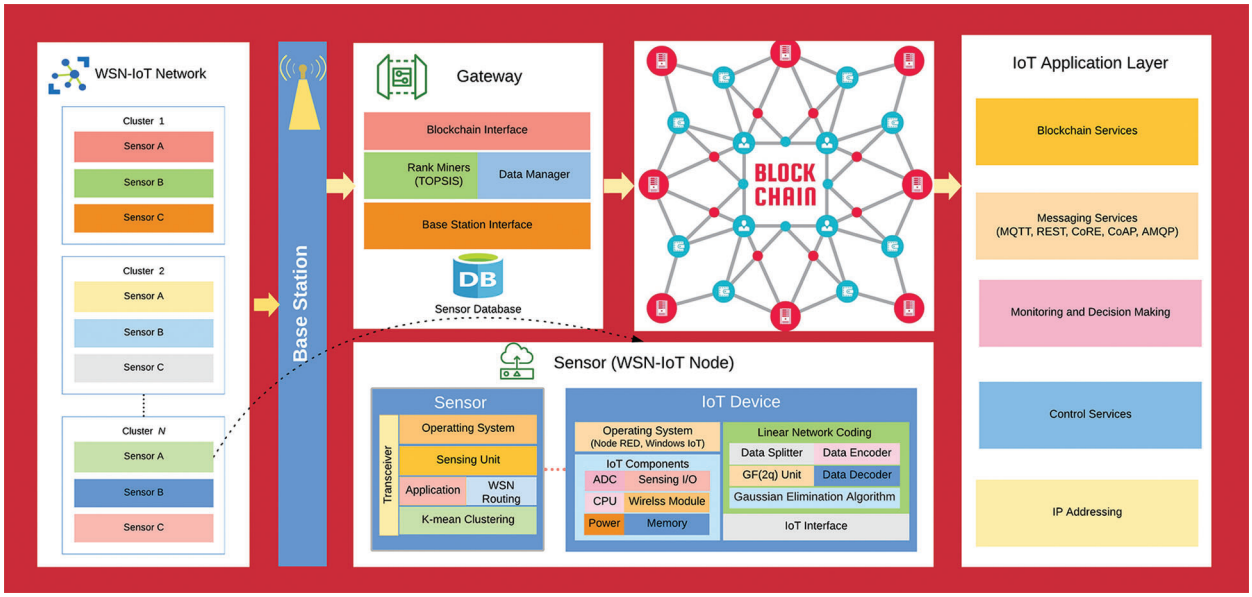

Figure 2: Architecture of the proposed WSNs model for smart cities

The energy consumption is measured by the Eqs. (1) and (2) using the first order radio model [31]. The transmission and the reception costs for the $L-bit$ message in the network is computed using the below Eqs. (1) and (2) [31].

$$E_T(L,d) = \begin{cases} L\left(E_e + \varepsilon_{fs} d^2\right), & d < d_{th} \\ L\left(E_e + \varepsilon_{mp} d^4\right), & d \geq d_{th} \end{cases} \tag{1}$$

$$E_R(L) = LE_e \tag{2}$$

where : $d_{th}-$ threshold distance

Energy, E_e denotes the electronic energy, which is dependent on the factors like the scattering and the coding of signals, the modulation and the filtering techniques, while $\varepsilon_{mp} d^4$ or $\varepsilon_{fs} d^2$, relies on the distance to the receiving node as well as the tolerable rate of the bit-error. The distance threshold is denoted by d_{th}. Energy dissipation can be expressed as Eq. (3) [31].

$$d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \tag{3}$$

3.2 K-means Clustering

K-means clustering is based on the Euclidean distances and CHs rely on the nodes' residual energies [32]. In this algorithm, the central node, which is responsible for collecting information about the node

such as the identification number (ID), the residual energy, and the positions of all the sensor nodes, saves these data in the form of a list. Once all the information is obtained from all nodes and then, the clustering algorithm (K-means) is executed [33].

Algorithm:

Step 1. Initially, to form 'k' clusters, let initially assume 'k' centroids which are placed at random places.
Step 2. Compute the Euclidean distance to all centroids from each node, and assign it to the nearest centroid as shown in Eq. (4). These 'n' initial clusters are generated, assuming that 'n' nodes are given which belongs to R_d.

Now, find the k centroids $\{m_i\}_{i=1}^{n}$ in R_d
s. t.

$$\frac{1}{k} \times \sum \left(\min_i d^2 \left(X_j, m_i \right) \right), \text{ for j} = 1 \text{ to k} \tag{4}$$

where:

$d\left(X_j, m_i\right)$ – Euclidean distance between X_j and m_i
$\{i\}_{j=1}^{n}$ – Centroid of the cluster

Step 3. Now, recompute the locations of centroids of all the clusters and check if there is a variation in the location from the earlier one.
Step 4. If changes are found then go back to Step 2, otherwise finalize the clusters and end the process of clustering.

3.3 Linear Network Coding

In linear coding, the data are split in many blocks by the source node. Every block contains m packets which are called as native packets [34,35]. This is represented by $x_j, \ \varepsilon\{1, 2, \ldots, m\}$. Thus; the LNC coded packet x_i' is transmitted by the source node to the next CH. This packet x_i' can be mathematically represented by the Eq. (5) [34].

$$x_i' = \sum_{j=1}^{m} c_{ji} x_j \tag{5}$$

where:

c_{ji}- matrix of coefficients

The operations like the multiplication and the addition are computed over a Galois Field, GF(2q) [34]. A code vector, $\overrightarrow{c_i} = (c_{i1}, c_{i2}, \ldots, c_{im})$ and the ID of the block are embedded into the x_i' header of the data packet. A counter that holds initial value of m' , where the value of m' is greater than m. This counter is maintained at the source node. The counter is decreased by one unit each time a coded packet is transferred to another node. The random transmission of the coded data packets continues till the value of the counter reaches to Zero [34]. The forwarding and recruiting functionalities are executed at each and every hop. The receiving CH starts the creation of the subsequent cluster once the packets of the same block are received. Now, this receiving cluster becomes a new transmitting cluster with the same nodes. The transmitting CH initially schedules the appropriate time of when the node is scheduled to send the encoded data to the receiver cluster which is applied to every nodes of the transmitting cluster [34]. The receiving CH then takes a control of the nearby nodes to form the receiver cluster, and to choose the nodes having the higher cost c_i. This variable c_i is defined for a node i, which can be possibly utilized for the receiver cluster, as expressed in the Eq. (6) [34,35].

$$c_i = \sum I_{ji}\left(1 - P_{ji}\right) \forall \textit{ node } i \in \textit{sending cluster} \tag{6}$$

where: P_{ji} – Probability of loss and

I_{ji} – Function of indication to indicate the availability of the sensor for receiving the packets.

The senor i might not be accessible because it is reserved to receive or to transmit data packets for another cluster from another path. The probability P_{ji} is intermittently tested by ping samples of every neighbors. I_{ji} relies on the way transmitting CH which assigns the sensor nodes to forward the data [34]. Consequently, the sensors which are expected to get more data are chosen as a recipient cluster from the transmitting cluster.

Let us consider that a node has obtained the encoded data x's. Then, the newly encoded data packet can be obtained from the Eqs. (7) and (8) [34,35].

$$x'' = \sum_{i=1}^{m} c_i x_i' \tag{7}$$

where:

c_i – Randomly generated numbers selected from GF(2q)

x'' – Native data packets

$$\begin{aligned} x'' &= \sum_{i=1}^{m} c_i \left(\sum_{j=1}^{m} c_{ij} x_j \right) \\ &= \sum_{j=1}^{m} \left(\sum_{i=1}^{m} c_i c_{ij} \right) x_i \\ &= \sum_{j=1}^{m} g_j x_j \end{aligned} \tag{8}$$

Similarly to the transmitting node, a sensor will embed a new code vector represented as $\vec{g}_i = (g_1, g_2, \ldots, g_m)$, within the x'' header of the packet, when transmitting the encoded data packet [34]. When the sink node gets an encoded data, it will initially check if the data is new. A data is considered to be new and fresh only if it is linearly independent from the data received previously from the same block that the sink node has received. If the encoded data is not new, the data will automatically be disposed. Therefore, as long as m new packets are gathered, the receiver node is capable of recovering the native data packets. The process of decoding at the sink node implicates solving the group of the linear equations using the Gaussian algorithm. The linear equation determines a unique solution if m is the rank of the matrix [34].

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_m' \end{pmatrix} \tag{9}$$

where:

$x'i$ - is an encoded packet

$(c_{j1}, c_{j2}, \ldots, c_{jm})$ - code vector

x_j - represents native packets.

The sensors in the transmitting cluster might has obtained two or more packets from the preceding cluster, such that, they can form their own combination as shown in Fig. 3. The sensor nodes merge all obtained packets from the same block using randomly chosen coefficients to create a random linear combination.

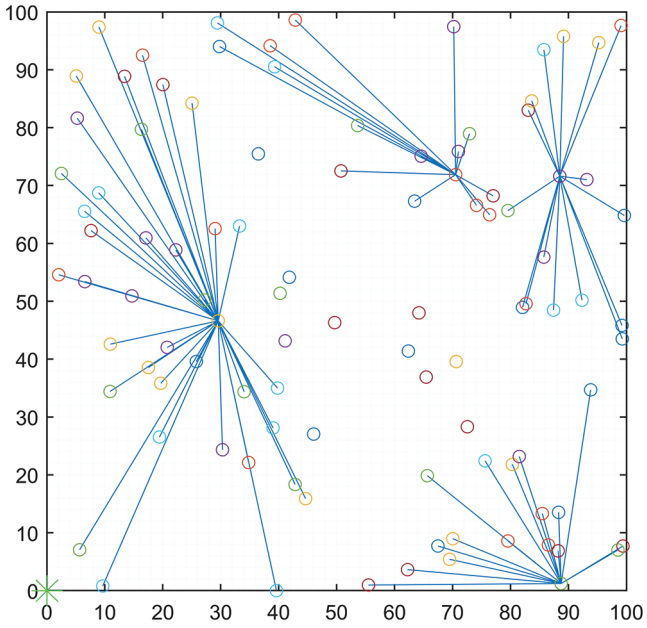

Figure 3: Data transaction in clusters

3.4 Blockchain Formation

The blockchain is a decentralized, distributed and immutable shared database record which contains the archive of the transactions and the assets [36–38]. The validated and timestamped data are transformed into blocks that are chained together. This blockchain employs Rivest-Shamir-Adleman (RSA) as well as SHA-256 algorithm for providing resilient cryptographic proof for the integrity and the authentication of data or information [39]. Generally, the data block comprises the list of communications and a hash-key to the preceding block. The centralized authorities and the trusted third parties (TTP) have high chance of getting interrupted, hacked, or compromised. In addition, they might as well disobey and turn into being corrupt in the near future, although they are trustable presently. Every transaction in the blockchain is a shared public record which is checked by a widely held consensus of the minority nodes that are energetically playing a role in the transaction's verifications and validations. The header field of the block comprises of several fields, out of which, one is a version for tracking the protocol upgradations. In addition, the header consists of a timestamp, the total count of communications, and the size of the block. Private blockchains are built, which include the sensors for saving the data and then sharing them. These nodes are then classified into the given two classes: non-mining nodes and mining nodes.

1) *Non-mining Nodes*-The purpose of the non-mining nodes is to only receive and broadcast the requests of data sharing transactions, therefore, it does not require the same quantity of resources when compared to a mining node. It is notable that all the nodes keep a complete and validated replica of the blockchain and the sensors with a respect to the smart contracts. It is assumed that all the CHs have a legit connection with the blockchain network and forever round of transactions, the sensors upload the data collected from the point of interconnects (PoIs) to the blockchain network. Thus, the total number of requests for data storage S sent by the nodes N, at the end of round r, is given as $S = N \times r$.

2) *Mining Nodes*-These nodes are utilized for verifying the transactions happening for the data sharing and for compiling them into the data blocks. These nodes are subjected to utilize the resources of machine computing consistently for the purpose of solving computational difficulties and for submitting the blocks to the blockchain network. Since each cluster head has a legit connection with the blockchain, the cluster head

can perform encryption on the data collected with a private key and then forwarding it with a signature to the blockchain like a request for the storage. Additionally, the cluster heads can transmit the request for a query to the blockchain and can collect the reverted data.

3) *Transaction and Consensus Mechanism*-The acquisition of a data packet from IoT devices or sensors triggers the creation of a blockchain transaction. The gateway performs a number of transactions including data, control, and outcome transactions that generate a large amount of data. Therefore, a reference pointer is stored to locate the data in the transaction on the blockchain. The typical format for a transaction includes the transaction identifier, the type of transaction, the reference to data, the address of the senders and receivers, the block number, the signature, the public and private keys. The selection of the healthy or the efficient blockchain nodes is an important aspect for a faster and reliable consensus algorithm. The healthy nodes which acts as a miner are selected based on multi-criteria which may include the parameters like the computing capability, the storage capacity, the reputation, the mining cost, the throughput and the bandwidth etc. In this work, to rank the reputation of the blockchain mining node, we have selected the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) [40,41]. Nowadays, proof-of-work (PoW) has become an important consensus mechanism to verify the transactions using the mathematical challenges. The mining node collects all the transactions pending to generate a block in the PoW and iteratively hashes the collected data with its hashes using the Merkle tree. The process of hashing terminates when the hash of transactions becomes equal to or less than a pre-determined target value (t_h) known as a threshold and shown in the Eq. (10) [40,41]. In this equation, H is SHA-256 hash function and b_c is the current block.

$$H(n \,||\, H(b_c)) \leq t_h \tag{10}$$

The probability to discover nonce of proof H can be expressed as the Eq. (11) [40,41].

$$P(H \leq t_h) = \frac{t_h}{2^{256}} \tag{11}$$

Upon successful computation of the target hash, the miner sends the proof to every node in the blockchain network, data transaction and other data to re-compute H by other miners to add the new block in the network. In this work, we have applied the consensus mechanism based on Rivest, Shamir and Wagner's time-lock puzzle as shown in below [42]. In the simulation, initially, 15 nodes have been generated as the blockchain nodes. As soon the number of new nodes is added in the sensor network, another configured blockchain is selected. The first configuration consists of 10 non-mining nodes and 5 mining nodes, while the second configuration consists of 50 non-mining nodes and 25 mining nodes. The last configuration consists of 100 non-mining nodes, while the number of mining nodes is 50. These mining nodes act for consensus mechanism.

Public:	$n = p\ q$
Private:	$\phi = (p-1)(q-1)$
$C \leftarrow CHAL(s, w)$	choose $c \in$ R [0, n)return (s, c, w)
$T \leftarrow MINT(C)$	compute $x \leftarrow H(s\|\|c)$ compute $y \leftarrow x^{x^w}\ (mod\ n)$ return (s, c, w, y)
$V \leftarrow VALUE(T)$	compute $x \leftarrow H(s\|\|c)$ compute $z \leftarrow x^w\ (mod\ \phi)$ if $x^z = y\ (mod\ n)$ return w else return 0

4 Results and Discussions

The suggested methodology was simulated in MATLAB R2018a an NS2 platform. This section of the research article provides all the results achieved from the simulation of the network transactions. The overall throughput, the alive nodes and the dead nodes for each round of transmission of the wireless communication are provided. The parameters considered for the simulation of the proposed network model are presented in Tab. 1.

Table 1: Simulation setup parameters

Parameters	Description	Value
N	Number of sensor nodes deployed in the network	100
A	Size of the square field	100 × 100 m
R_{max}	Maximum rounds	12000
i	Number of iterations for K-means algorithm	15
E_0	Initial energy	0.5 J
ϵ_{fs}	Amplifier energy spent in transmission when $d \leq d_0$	70 nJ/bit
ϵ_{mp}	Amplifier energy utilized in the data transaction when $d > d_0$	120 nJ/bit
C	Number of cluster heads selected	4
b	Size of data for one block	2000 bits

The proposed scheme uses LNC for the data transmission that enhances the energy efficiency of WSNs. The security of data [43] is established using the blockchain.

4.1 Performance Metrics

Average throughput analysis–The amount of data successfully obtained at the receiver end per unit time in the network. This can be expressed as a given in the Eq. (12).

$$Average\ throughput = \frac{number\ of\ packets\ received}{delay} \tag{12}$$

Network Lifetime–This can be defined as a relation between the consumed energy and the available energy in the network [44]. In other words, this refers to the time when the very first node exhausts its energy in the WSN.

Residual Energy–This refers to energy remnants in a node. The residual energy can be expressed in the Eq. (13).

$$E_r = \frac{E_{rem}}{E_{avg}} \times \frac{D_{max}}{D_{bs}},\ \text{where}\ E_{avg} = \frac{\sum_1^n E_{rem}}{n} \tag{13}$$

Reliability analysis–The reliability is the measurement of system life time that is inversely proportional to the loss of packets.

$$Reliability = 1 - \frac{t}{MTBF} \tag{14}$$

Packet delivery ratio (PDR) analysis–This can define as the percentage of the total packets obtained by the receiving end to the sum of the packets of the data sent.

$$PDR = \frac{sum\ of\ \ data\ packets\ received\ by\ receiver}{sum\ of\ \ data\ packets\ sent\ by\ transmitter} \tag{15}$$

4.2 Performance Evaluation

Fig. 4 displays the overall throughput obtained for increasing rounds of the data transmission. The total number of rounds of the transmissions is 12,000. The throughput reaches up to 700000 bits/second (bps). A comparison of throughput with the existing work has been presented in Tab. 2, which demonstrates the higher throughput achieved by the presented network model compared to the existing work.

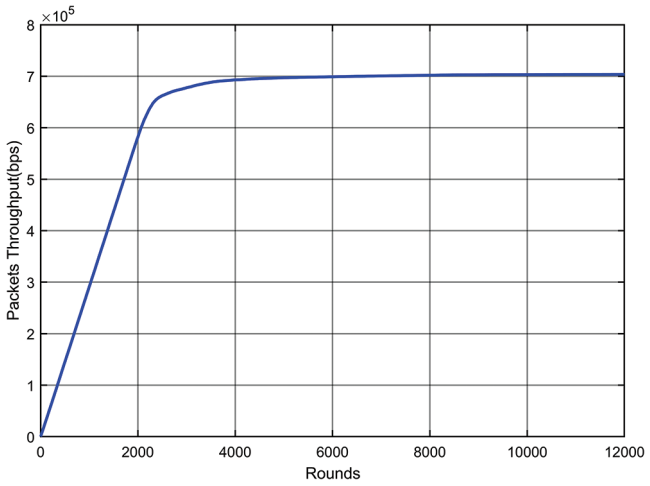

Figure 4: Throughput for increasing number of rounds

Table 2: Throughput analysis

Protocol	Throughput (bps)
EISEP [45]	237761
AWFCC [46]	30000
R-LEACH [47]	200000
I-LEACH [48]	20000
Proposed model	700000

In general, the data transmitting process of the wireless networks use CHs to receive the information and to send to BS. In this proposed network, CHs wait until the information is gathered and encoded via a linear network coding. A block is created before uploading onto the internet. In order to access the information, the block connections of the blockchain have to be decoded with the help of the previous hash key used in the linear network coding. This ensures a reliable data transmission of IoT devices. A related comparative analysis with the existing work [46] has been shown in Tab. 3.

Table 3: Reliability analysis

Protocol	Reliability
AWFCC [46]	0.97
Proposed model	0.99

Fig. 5 displays the alive and dead nodes for varying number of transmission rounds. It can be seen in Fig. 5, that at the round 12,000, there are still 4 nodes staying alive. This infers that the energy spent for the transmission is drastically reduced in the proposed WSNs. Similarly, in Fig. 6, it can be seen that 96 nodes are dead at the 12,000 transmission rounds. Tab. 4 presents the lifetime comparison of the work proposed in this paper with the work proposed in the existing literature. From Tab. 4, clearly demonstrates that the lifetime of the proposed network is improved comparing to the existing works.

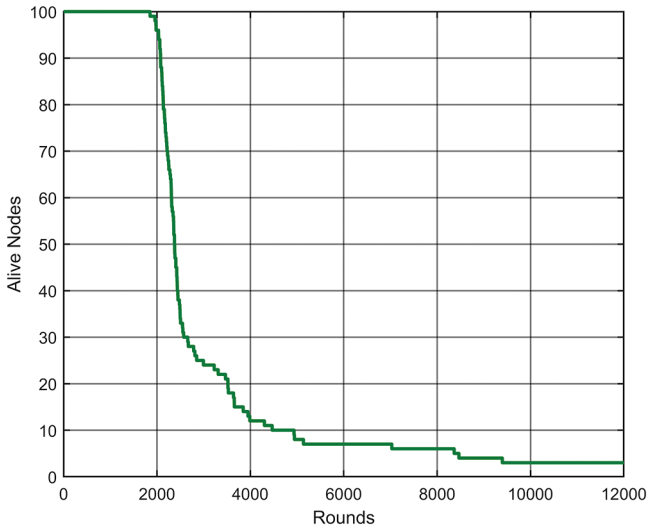

Figure 5: Alive nodes for the proposed network

Fig. 7a displays the average residual energy of the WSN. In the methodology presented, the initial energy is not completely exhausted even after 12000 rounds of the data transmission. Fig. 7a illustrates the low energy consumption which may prevents the network failures; thus, the increases of the network lifetime is guaranteed.

In WSNs, if the PDR is high, all the information is obtained by the receiving node without any loss of the packets. In Fig. 7b, PDR is high for differing intervals of time (increasing number of rounds of data transmission). The graph clearly shows that the proposed model has 99.98% PDR even after 12,000 rounds, which is better than the existing work [49].

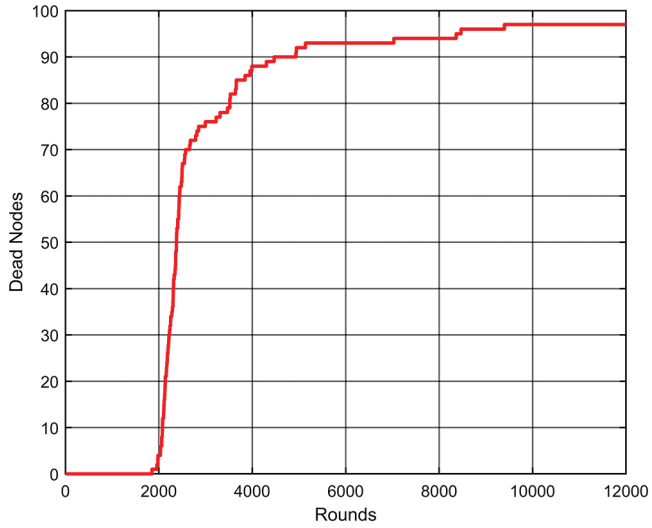

Figure 6: Dead nodes for the proposed network

Table 4: Lifetime comparison

Protocol	First node dead	Last node dead
EISEP [45]	1203	13990
AZ-SEP [49]	850	8000
R-LEACH [47]	1382	2474
I-LEACH [48]	98	1700
PE-LEACH [50]	1265	1926
Proposed model	1772	10000

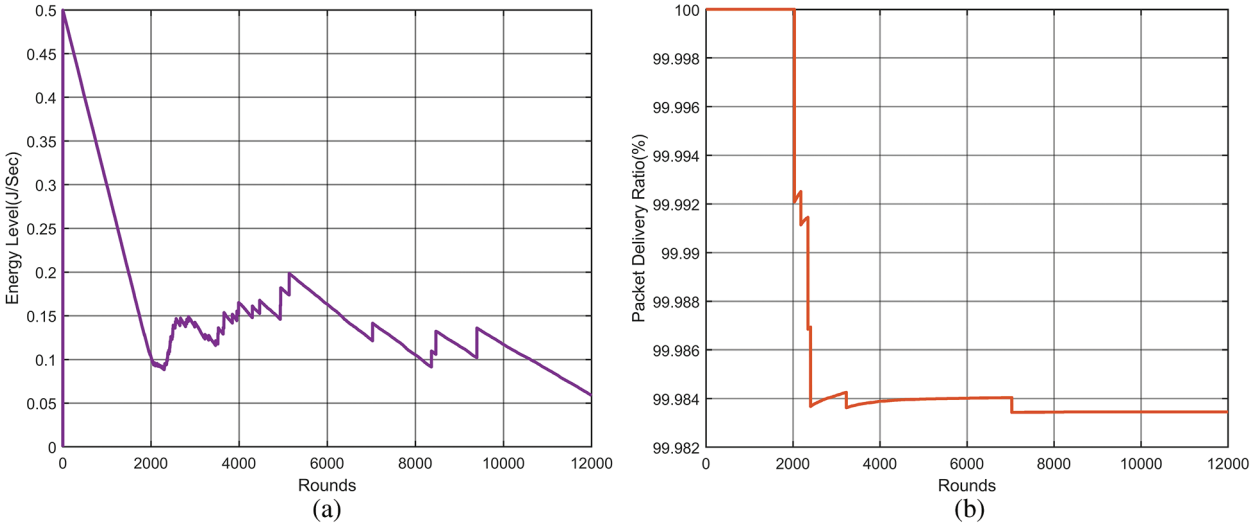

Figure 7: Average residual energy and Packet delivery ratio. (a) Average residual energy and (b) Packet delivery ratio

5 Conclusion

This paper has proposed a K-means clustering combined with the linear network coding for WSN with the blockchain enabled IoT devices. The cluster heads are selected using K-means clustering algorithm based on the spent energy and the distance from the base station. The data from the cluster heads undergoes a linear network coding before the communicating with the sink node. In this way, all the nodes have a direct communication with BS; therefore, the energy is conserved to a greater extent. Conservation of the energy subsequently extends the lifespan of the sensor network. The presented model is evaluated with the respect to the number of the live nodes, the packet delivery ratio, the throughput, the consumption of the energy and the reliability. It is found that the efficiency of the proposed network model is superior in the comparison with the other existing techniques. The comparative results prove that the suggested scheme performs more efficiently compared to the existing models. In the future, this work can be applied for MANETs and VANETs where the nodes are mobile.

Funding Statement: This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fasttrack Research Funding Program.

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

References

[1] J. Jin, J. Gubbi, S. Marusic and M. Palaniswami, "An information framework for creating a Smart City through Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 112–121, 2014.

[2] B. N. Silva, M. Khan and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustainable Cities and Society*, vol. 38, pp. 697–713, 2018.

[3] M. T. Lazarescu, "Design of a WSN platform for long-term environmental monitoring for IoT applications," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 45–54, 2013.

[4] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] Y. K. Chen, "Challenges and opportunities of the Internet of Things," in *17th Asia and South Pacific Design Automation Conf.*, Sydney, NSW, Australia, pp. 383–388, 2012.

[6] A. P. Abidoye and I. C. Obagbuwa, "Models for integrating wireless sensor networks into the Internet of Things," *IET Wireless Sensor Systems*, vol. 7, no. 3, pp. 65–72, 2017.

[7] S. Bansal and D. Kumar, "IoT Ecosystem: A survey on devices, gateways, operating systems, middleware and communication," *International Journal of Wireless Information Networks*, vol. 27, pp. 340–364, 2020.

[8] M. C. M. Thein and T. Thein, "An energy efficient cluster-head selection for wireless sensor networks," in *Int. Conf. on Intelligent Systems, Modelling and Simulation*, Liverpool, UK, pp. 287–291, 2010.

[9] F. Haleem, B. Jan, H. Javed, N. Ahmad, J. Iqbal *et al.,* "Multi-criteria-based zone head selection in Internet of Things based wireless sensor networks," *Future Generation Computer Systems*, vol. 87, pp. 364–371, 2018.

[10] M. A. Matin and M. M. Islam, "Overview of wireless sensor network," in *Wireless Sensor Networks-Technology and Protocols*, M. A. Matin, IntechOpen, London, UK, pp. 1–3, 2012.

[11] M. Handy, M. Haase and D. Timmermann, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection," in *4th Int. Workshop on Mobile and Wireless Communications Network*, Stockholm, Sweden, pp. 368–372, 2002.

[12] A. A. Ahmed and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14–15, pp. 2826–2841, 2007.

[13] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," *IEEE INFOCOM 2003*, vol. 3, pp. 1713–1723, 2013.

[14] S. M. Bozorgi and A. M. Bidgoli, "HEEC: A hybrid unequal energy efficient clustering for wireless sensor networks," *Wireless Networks*, vol. 25, no. 8, pp. 4751–4772, 2019.

[15] R. Zhang, J. Pan, D. Xie and F. Wang, "NDCMC: A hybrid data collection approach for large-scale WSNs using mobile element and hierarchical clustering," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 533–543, 2016.

[16] H. Taheri, P. Neamatollahi, O. M. Younis, S. Naghibzadeh and M. H. Yaghmaee, "An energy-aware distributed clustering protocol in wireless sensor networks using fuzzy logic," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1469–1481, 2012.

[17] J. Gnanambigai, N. Rengarajan and K. Anbukkarasi, "Leach and its descendant protocols: A survey," *International Journal of Communication and Computer Technologies*, vol. 1, no. 3, pp. 15–21, 2012.

[18] J. P. Hu, Y. H. Jin and D. Liang, "A time-based cluster-head selection algorithm for LEACH," in *ISCC IEEE Sym. on Computers and Communications*, Marrakech, Morocco, pp. 1172–1176, 2008.

[19] F. Xiangning and S. Yulin, "Improvement on LEACH protocol of wireless sensor network," in *Int. Conf. on Sensor Technologies and Applications, SensorComm*, Valencia, Spain, pp. 260–264, 2007.

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

[21] D. Suresh and K. Selvakumar, "Energy efficient double cluster head selection algorithm for WSN," *Journal of Theoretical & Applied Information Technology*, vol. 58, no. 2, pp. 372–380, 2005.

[22] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[23] J. Duan, D. Gao, D. Yang, C. H. Foh and H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 58–69, 2014.

[24] S. Sharma, D. Sethi and P. P. Bhattacharya, "Artificial neural network-based cluster head selection in wireless sensor network," *International Journal of Computer Applications*, vol. 119, no. 4, pp. 34–41, 2015.

[25] S. S. Jamadar and P. D. Y. Loni, "Efficient cluster head selection method based on k-means algorithm to maximize energy of wireless sensor networks," *International Research Journal of Engineering & Technology*, vol. 3, no. 8, pp. 1579–1583, 2016.

[26] R. J. Hwang and Y. Z. Huang, "Secure data collection scheme for wireless sensor networks," in *2017 31st Int. Conf. on Advanced Information Networking and Applications Workshops*, Taipei, pp. 553–558, 2017.

[27] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma *et al.,* "Research on trust sensing based secure routing mechanism for wireless sensor network," *IEEE Access*, vol. 5, pp. 9599–9609, 2017.

[28] B. T. Mayee, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand *et al.,* "Residual energy-based cluster-head selection in WSNs for IoT application," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5132–5139, 2019.

[29] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao *et al.,* "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5791–5802, 2019.

[30] G. Jingjing, B. Sun, X. Du, J. Wang, Y. Zhuang *et al.,* "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018.

[31] 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, pp. 1–10, 2000.

[32] H. Harb, A. Makhoul, D. Laiymani, A. Jaber and R. Tawil, "K-means based clustering approach for data aggregation in periodic sensor networks," in *IEEE 10th Int. Con. on Wireless and Mobile Computing, Networking and Communications*, Larnaca, pp. 434–441, 2014.

[33] P. A. Forero, A. Cano and G. B. Giannakis, "Distributed clustering using wireless sensor networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 4, pp. 707–724, 2011.

[34] Z. J. Haas and T. Chen, "Cluster-based cooperative communication with network coding in wireless networks," in *2010 - MILCOM 2010 Military Communications Conf.*, San Jose, CA, pp. 2082–2089, 2010.

[35] S. Y. R. Li, R. W. Yeung and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003.

[36] X. Wang, P. Zeng, N. Patterson, F. Jiang and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45061–45072, 2019.

[37] G. Rathee, A. Sharma, R. Kumar and R. Iqbal, "A Secure communicating things network framework for industrial IoT using blockchain technology," *Ad Hoc Networks*, vol. 94, no. 1, 101933, 2019.

[38] 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. 241–251, 2020.

[39] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Thing," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[40] C. L. Hwang and K. Yoon, *Multiple Attribute Decision Making: Methods and Applications*. New York: Springer-Verlag, 1981.

[41] V. Balioti, C. Tzimopoulos and C. Evangelides, "Multi-criteria decision making using TOPSIS method under fuzzy environment. application in spillway selection," *Proceedings*, vol. 2, no. 11, pp. 2–8, 2018.

[42] B. Adam and Hashcash, "A denial of service counter-measure," 2002. [online]. Available: http://www.hashcash.org/hashcash.pdf.

[43] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[44] R. Kandpal and R. Singh, "Improving lifetime of wireless sensor networks by mitigating correlated data using LEACH protocol," in *1st India Int. Conf. on Information Processing*, Delhi, India, pp. 1–6, 2016.

[45] S. D. Kumar, S. Bagga and R. Rastogi, "Energy efficient improved SEP for routing in wireless sensor networks," S. K. Bhatia, S. Tiwari, K. K. Mishra and M. C. Trivedi (eds.), in *Advances in Computer Communication and Computational Sciences*. vol. 924. Singapore: Springer, pp. 143–152, 2019.

[46] S. Vikas, S. Tripathi and K. Singh, "Energy efficient optimized rate-based congestion control routing in wireless sensor network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1325–1338, 2019.

[47] M. Ni, L. Yang, Y. Zhou, L. Jiang and H. Hu, "An Effective cluster heads selection method for wireless sensor networks," in *2018 IEEE 4th Int. Conf. on Computer and Communications*, Chengdu, China, pp. 928–933, 2018.

[48] T. M. Behera, U. C. Samal and S. K. Mohapatra, "Energy-efficient modified LEACH protocol for IoT application," *IET Wireless Sensor Systems*, vol. 8, no. 5, pp. 223–228, 2018.

[49] F. A. Khan, M. Khan, M. Asif, A. Khalid and I. U. Haq, "Hybrid and multi-hop advanced zonal-stable election protocol for wireless sensor networks," *IEEE Access*, vol. 7, pp. 25334–25346, 2019.

[50] H. Mohapatra and A. K. Rath, "Fault tolerance in WSN through PE-LEACH protocol," *IET Wireless Sensor Systems*, vol. 9, no. 6, pp. 358–365, 2019.