International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I11P230

Volume 70 Issue 11, 277-287, November 2022
© 2022 Seventh Sense Research Group®

Original Article

A Novel Method for Enhancing the Network Lifetime using Energy-Efficient Routing Protocol Approach for Wireless IoT Sensor Network Applications

Battina Srinuvasu Kumar[1], S.G. Santhi[2], S. Narayana[3]

[1,2]*Department of Computer Science & Engineering, Annamalai University, India.*
[3]*Department of Computer Science & Engineering, SR Gudlavalleru Engineering College, Gudlavalleru, India*

[1]*Corresponding Author : bskdata@gmail.com*

Received: 01 July 2022 Revised: 30 August 2022 Accepted: 16 November 2022 Published: 26 November 2022

Abstract *- The Internet of Things (IoT) profoundly impacts our daily lives, from tiny wearable gadgets to enormous industrial systems. As a result, a wide range of IoT applications has been designed and implemented utilizing several IoT frameworks. Rules, protocols, and standards that guide the development of IoT applications may be found in an IoT framework. The success of these applications is mostly dependent on the ecosystem features of the IoT framework, with the primary focus being placed on the security procedures that are incorporated into the framework. It is because concerns about security and privacy are of the utmost importance. End-to-End encryption is not being ensured during data transfer in IoT due to several issues. Cyberattacks are easier to launch since most IoT devices utilize default login credentials and are not correctly configured or protocoled. In order to maintain high levels of security, not all IoT devices can be equipped with the latest security measures. On the other hand, the rising interconnectedness of common things might provide hackers with a bunch of new attack routes. Low-cost IoT devices have a wide range of capabilities and resources, making it challenging to deploy traditional perimeter defenses in a dynamic IoT environment. The authors of this research considered all of this while creating a routing method for wireless IoT sensor networks that is simple yet efficient in terms of energy consumption. This article uses an optimization problem to simulate the energy constraint problem of IoT devices. The suggested protocol uses clustering, cluster head election, and computing the least energy-expensive path to provide efficient and real-time Routing. This helps reduce the amount of power wasted by individual devices. Communication intent among transmitter and receiver devices is characterized using a route computation equation. The clustering algorithm's characteristics have been chosen to maximize energy conservation efforts. In addition, this article employs an evolutionary sleep scheduling approach that may be utilized to enhance network performance further. Particle Swarm Optimization (PSO) and Genetic Algorithm (G.A.) are combined in this method (G.A.). As a result of these simulations, the proposed routing protocol was compared to two current routing protocols on metrics, including the number of active nodes and energy dynamics. According to the simulation findings, the suggested protocol beats both LEACH and FCM in terms of performance.*

Keywords - *IoT security, Routing protocol, Network applications, Cyberattacks, Energy efficiency, Network lifetime.*

1. Introduction

The Internet of Things (IoT) significantly impacts every area of our day-to-day activities. In addition to healthcare and transportation, it also includes entertainment, industrial equipment, footwear, and residences. IoT's pervasiveness eases various routine activities, enhances how individuals engage with the environment and surroundings, and enhances our social relationships with other people and items [1].

This comprehensive view, on the other hand, poses specific issues, such as what level of security might be provided by the Internet of Things and the manner in which it ensures and safeguards the privacy of its customers. Distributed computing is extremely complicated, and there are no common principles or frameworks to ease high-level implementation and many programming languages and communication protocols.

Developing apps for the IoT might be a complex process because of these factors. All functional and non-functional software needs must be met by developers who manage the infrastructure and handle both software and hardware layers. As a result of this increased complexity, the new Internet of Things (IoT) programming frameworks has emerged quickly [2].

The Internet of Things (IoT) is a technology that detects and collects data from devices worldwide (IoT). Several network devices are spread around the country to monitor such information. The internet may transfer data to the appropriate application or user. Using this technology, intelligent machines can communicate and interact with other items distributed in the environment. Individuals today employ a variety of communication channels to connect and interact with one another [3]. The internet is widely acknowledged as the most commonly used means of communication in the world today. Since it has enhanced people's quality of life, it has been increasingly popular with researchers and companies alike during the last two decades. In order to provide the best service as a whole, several things function together rather than independently. This technique is quite helpful in a variety of real-world situations. The Internet of Things (IoT) may be used to build a smart home that automatically closes the windows when the air conditioning is switched on [4].

People with disabilities can benefit from the Internet of Things (IoT) in times of need since this technology can create a whole cooperative system by linking gadgets. The Internet of Things (IoT) offers a wide range of sophisticated software and connectivity services. Items are linked to each other or other objects via these networks. This page provides access to the media found inside these networks. They also aid in the exchange of information between different items. Each object in this scenario must be a component of the little computer. The various projections provided here have been surpassed by the microchip via which the link is made. RFID, sensors and actuator, miniaturization, nanotechnology, and smart entities are a few of the technologies at play here [5]. The substructure of an IoT scenario is understood to have greater computing power. Even the tiniest components in a computer network have this kind of power. IoT devices use RFID and sensors currently used in various technologies to connect to the outside world (see Fig. 1).

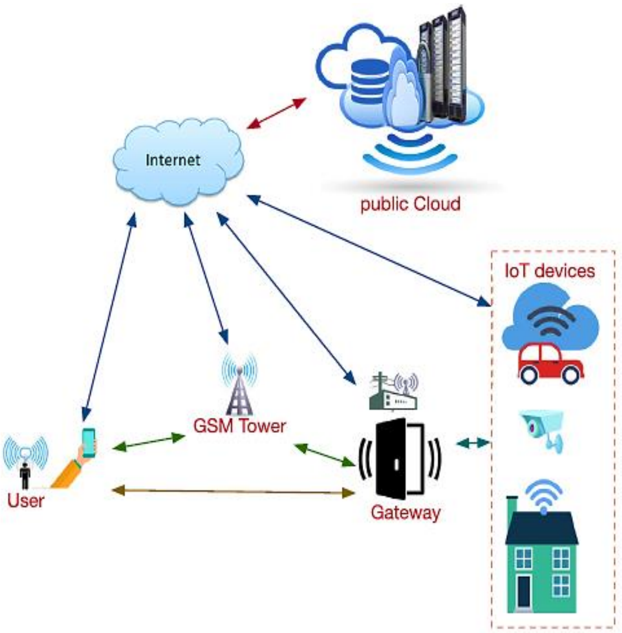

Fig. 1 A high-level IoT system model

Choosing the best path for data transmission is a difficult problem that the routing protocol strives to accomplish. Network elements such as channel characteristics, network type, and performance measures [6] all play a role in determining the best path to take. B.S. and S.N.s are closer together in smaller IoT networks. Therefore communication can take place in a single hop. Direct connection with the B.S. may not be possible in large-scale IoT networks; therefore, communication occurs via many hops. Radio power, bandwidth, energy, or memory [7] are all possible culprits. With the use of hierarchical routing techniques, wireless sensor networks (WSNs) can achieve higher network performance and longer battery life. Even so, the authors presented a cluster-based optimization that centralizes energy efficiency [8], scalability [9], complexity [10], and resilience [5] in order to obtain greater energy efficiency. An optimization model with several objectives, such as particle swarm optimization–genetic algorithms, can improve the efficiency of hierarchical clustering.

To save energy, it is necessary to optimize the lifetime of a network in WSNs, which has piqued the interest of several researchers [11]. One way to measure network life span is to look at how long it takes for the first sensor node to lose all of its energy. Researchers have attempted to improve many factors, such as hop count, path dependability, and energy consumption, to maximize the network's lifetime. The authors of this research sought to extend the network's lifespan by enhancing the routing protocol, increasing the hop count, and establishing a more dependable path. According to the authors' plan, elements such as residual energy, hop count, and a dependable path to the sink were employed to enhance network life expectancy. Metrics like throughput, energy usage, and packet delivery were used to verify the approach's performance.

Several strategies may be used in conjunction with the routing protocol to save energy [12]. A sleep schedule is an example of this. Idle devices waste a lot of energy, which is why sleep scheduling is so common in WSNs. This method puts devices to sleep (turn them off) at predetermined intervals based on a preset measure. In an IoT-based WSN, there are a number of sleep scheduling algorithms that may be used. Approaches based on evolutionary algorithms, such as [14], which uses a Particle Swarm Optimization-inspired sleep scheduling strategy for WSNs, have shown encouraging results. Genetic Algorithm (G.A.) [15] and Particle Swarm Optimization (PSO) [29] are two well-known evolutionary approaches used in this study for the aim of sleep schedule.

To summarise, the following are the paper's main contributions:

- An IoT energy optimization challenge in the form of green Routing.
- Minimal energy (MINEN) routing protocol was developed to solve the optimization challenge.

- Enhancing the energy-saving effort by adding a sleep scheduling mechanism to the minimal energy routing protocol, GSO.
- A comparison of the proposed protocol's performance with two commonly used routing protocols and a variety of sleep scheduling methods.

The rest of the paper is laid out in this way. Section 2 provides a literature survey. A methodology was discussed in Section 3. Section 4 explains how the proposed routing protocol works; the simulation is described, as well as the outcomes that it yielded. Section 5 includes the scope for further research and the conclusion.

2. Literature Survey

IoT-related research has been going on a lot recently. System enhancement and smart cities are becoming more commonplace due to the Internet of Things (IoT). Prior research on the Internet of Things (IoT) may be divided into three broad categories: industrial, security, and logistics. Industrial IoT research is primarily concerned with increasing the effectiveness of operating systems and administration. Regarding integrating IoT infrastructure into a supply chain management system, the author in [16] examined and proposed strategies for overcoming potential roadblocks and issues and considerations for long-term success in the field. In [17], a concept was developed to minimize medical institutions' operational costs by integrating IoT services in a cloud environment and improving service quality utilizing the Internet of Things. In order to efficiently maintain cattle buildings, [18] designed an IoT-based system. An additional method for increasing user profitability and the efficiency of livestock house operations were proposed: gathering livestock data in the cloud and determining the best time to trade.

In constrained Routing, the author in [19] proposed a delay-aware and energy-efficient opportunistic node selection (DA-EEORR). The authors say their proposed approach is unique and well-suited for use in a time-critical setting. The suggested approach finds an ideal path to strike a favourable compromise between energy consumption and average end-to-end latency. An opportunistic random graph (OCRG) is used to select the next hop in the model. Aside from transmission frequencies, residual energy, connection quality, and so forth, OCRG is utilized to compute optimal path connectivity. In order to discover the next-hop node with the shortest distance, the suggested model used the idea of confined research space. This approach is superior to existing standards, according to the results of a simulation. The proposed technique outperforms the alternatives in terms of network lifetime, power consumption, the overhead of the control packet, and packet delivery ratio. There were just a few significant discoveries because the study concentrated more on course correction and tracking routes rather than determining the best path in a hierarchical network. Achieving a good balance between energy consumption and delay is achieved in the presented work, but it may yet be developed to include many sink nodes for practical delay-sensitive applications.

The author has studied wireless body area networks (WBANs) [20]. (WBANs). For example, WBANs have been used extensively in remote patient monitoring, sports activity monitoring, and so on. WBANs are networks of wearable sensors and computers that transfer the detected data around a human body. An electrocardiogram (ECG), an electroencephalogram (EEG), and other critical bodily parameters may be monitored using them. As WBANs are limited in resources, they require adequate and energy-efficient routing techniques. WBANs can benefit from an energy-efficient and reliable routing method (ERRS) developed by [40]. The proposed technique implements two solutions: the forwarder nodes' selection and rotation. EERS uses adaptive static clustering routing to extend the network's lifespan and increase its stability. The EERS showed a 26% improvement over conventional methods in simulations. Throughput and network stability are used to evaluate the EERS' performance. Furthermore, the suggested algorithm outperformed the SIMPLE and M-ATTEMPT protocols regarding end-to-end latency by 17% and 40%, respectively. For WBANs to be widely deployed, researchers need to address issues such as WBANs' scalability and mobility, which were handled in the simulation but remain issues in real life.

For unattended time-sensitive nodes, [22] also highlighted the need for extended network lifetimes and rapid data transfers. Most routing algorithms for these kinds of applications fail to take into account network traffic, packet loss, and energy usage, according to the authors of the research. The authors also note the requirement for a homogenous sensor network since real-world deployments must deal with a wide range of nodes, [23] has presented a new method for dealing with these issues, which is called delay-aware energy efficient reliable Routing (DA-EERR). The suggested method specifies a restricted search area to ensure the timely transmission of time-sensitive data. A delay-aware, energy-balanced path is then selected by an algorithm inside the search space, ensuring quick communication between the source and sink. Data packets from big networks will have a better chance of being successfully received using the proposed strategy.

The research community paid close attention to IoT security and privacy concerns and addressed them on several levels. Using four distinct lenses, the authors of [24] examined the security and privacy problems surrounding the Internet of Things. To begin, they discuss the drawbacks of implementing security in IoT devices (such as battery life and processing power) and possible workarounds (e.g., lightweight encryption scheme designed for embedded systems). Second, they provide an overview of the various IoT attack classes (e.g., physical, remote, local, etc.). Authentication and authorization systems are the third areas of concentration for these researchers. For their final analysis, they examine security vulnerabilities at several levels (e.g., physical, network, etc.). [25,26] and examined the security and privacy vulnerabilities in IoT at each layer specified in the 3-layer architecture [27,28] and reviewed most of the security weaknesses present in IoT, which arose from the different communication technologies utilized in wireless sensor networks. It is suggested in [29] that an authorization access model be used to provide access control, and only authorized users can utilize the IoT.

A team of researchers has discussed IoT middleware security vulnerabilities [30] and found that many current systems rely on middleware frameworks for their security features. Middleware approaches are analyzed and evaluated based on known security and privacy issues, and the authors illustrate how each solution handles security. The study concludes with a list of needs for secure IoT middleware. These polls all focus on a single aspect of the common IoT security standards (e.g., network protocols or middleware employed). No previous studies have examined IoT security from a programming level. Thus we believe this is the first time that a subset of commercially available IoT programming frameworks has been evaluated for security.

Sensor nodes are identified by their position in location-based routing systems such as [31], [32]. Several ways to accomplish this goal include signal strength measurements, information sharing, and GPS tracking. A protocol's last subcategory has to do with conserving energy. An efficient method of delegating the routing tasks based on network device capabilities is hierarchical Routing [33], [34], [35], [36]. Data processing and data transport are the responsibilities of high-energy nodes, whereas environmental sensing is the responsibility of low-energy devices. When data processing and transmission are delegated to certain cluster heads, they are considered part of hierarchical Routing. According to this paper's routing system, sensors are grouped together according to various important factors, including their distance from the base station, remaining battery levels, message length, and data collected by the sensor nodes.

For transferring data to the base station, LEACH is a hierarchical routing system that uses the clustering of devices. Cluster heads are in charge of aggregating, processing, and communicating data in the cluster. Cluster heads are randomly rotated to distribute the protocol's routing burden among several sensors. Reducing the amount of data that must be communicated is another goal of data fusion and aggregation. An energy-efficient sensor network routing technique commonly used is LEACH. Thus we use it as a starting point for our strategy.

Other energy-efficient strategies have been advocated in the past: Data is routed to the nearest neighbour nodes using the MTE protocol (Minimum Transmission Energy) [38]. Using MTE, however, the nodes near the base station are overwhelmed with routing-related processing load and run out of energy extremely quickly. In various protocols, such as LEACH and FCM [39], the uneven allocation of routing work has been alleviated using collaborative Routing.

There are also some downsides to LEACH. Random rotation of cluster heads may result in multiple times of communication that are less than optimum. An incompetent node might choose a cluster head during these periods. As a second consideration, the distances between the cluster nodes in the network are not all the same. Therefore, some nodes would have to send data across more considerable distances than others. We account for these two issues when we suggest a technique that elects cluster heads based on device battery levels. Furthermore, all cluster heads in the network work together to send data to the base station. A route composed of all of the cluster's nodes' heads is calculated for the ultimate data transfer.

FCM [1] is a clustering-based routing technology that uses a similar approach. Based on the Euclidean distance between devices and cluster centres, FCM offers grouping. It is done to ensure that the cluster's sensor nodes all use the same amount of energy. Based on residual energy levels, cluster chiefs in FCM are elected. Some cluster heads collect information from the network's devices and send it to a base station. No consideration of device data generating capacity in cluster creation by FCM. As a result, if the majority of devices that create long messages and actively detect larger amounts of data than others are grouped together, the designated cluster head of this group would consume more energy than the others in the network. The battery life of this cluster would be shorter than the others over time. With this shortcoming in mind, our protocol considers three device characteristics for cluster formation: the number of sensors in a cluster, the distance of nodes from their base station, and the length of messages that devices send. A simulation and comparison of our proposed routing protocol with LEACH and FCM are shown in Section 4. Based on a number of measures, it is going to become clear that our protocol performs better than LEACH as well as FCM.

3. Methodology

This section discusses the WSN routing method that uses PSO and G.A. The PSOGA technique consists of two parts. When it begins, it obtains the population for a specified number of generations and holds the M strongest people. Selection, crossover, and mutation are used in the second phase to create the number of individuals excluded in the first phase. A combination of PSO and G.A. is used to populate the following generation, with these M individuals and newly created individuals. As a result, the proposed method's PSO and G.A. lead to high convergence rates and global optimum. Over the course of each generation, the number of the fittest people is steadily increased by this method. In order to get a better grasp of the proposed technique, we first explore the PSO and G.A. approaches.

3.1. Genetic Algorithm Search-Based Routing

The genetic algorithm (G.A.) is a search-based optimization strategy that uses natural selection and genetic inheritance principles [27–29].

Table 1. Network layer attack

Attack	Technique & Implications	Defence Mechanism
Eavesdrop	As a result, an opponent can listen to or change the data that is being sent [26].	A new approach to VLC, based on channel correlation and error estimates, is both novel and practical [27].
Resource Consuming Attacks	Inequity, Collision, and Exhaustion are all forms of assault. Failure to meet customer expectations.	TLS is used to implement many layers of security [39].
Modification-type attacks (Routing attacks)	Attacks from the "grey hole," "sinkhole," "black hole," and "wormhole" [28]. Authentication and access control methods included in the system cannot prevent or detect these attacks.	An IDS is designed to detect sinkholes and selective forwarding attacks [31].
		IDS in an IoT context to identify wormhole attacks [30].
		Security breaches and malicious conduct may be detected using the RPL protocol's specification-based approach [29].
Sybil attack	False identity, DoS, or replay threat [32] of a node.	Host-based and SDN-based IDS disables the victim's device. SAAS (software as a service) [4].
Denial-of-Service Attack	An ICMP Broadcast is also known as an ICMP Denial of Service (DDoS) or a Denial of Sleep (DOS) [1].	Port scanning and DDoS detection using SDN architecture [37]. IDS provides better security in conjunction with each other.
		The gradient-based technique helps minimize ML IDS evasion threats [38].

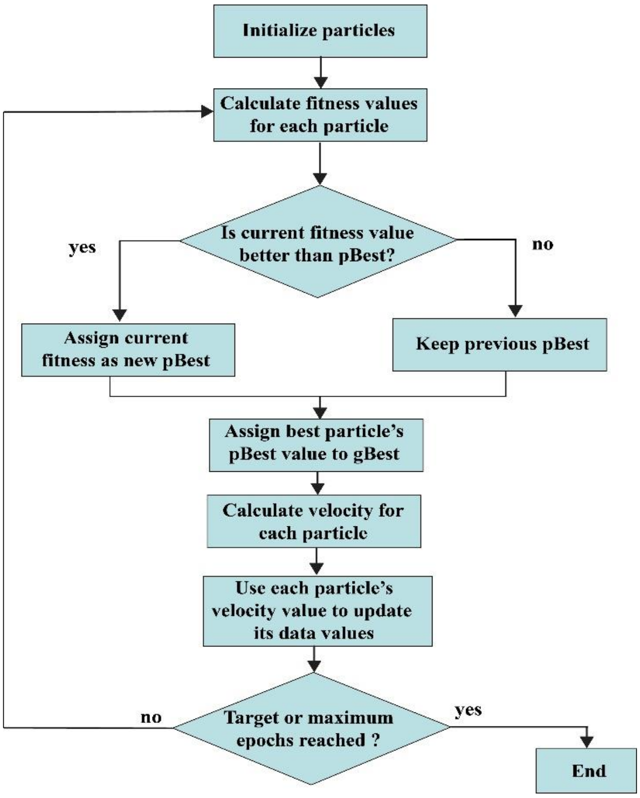
Initialize particles
Calculate fitness values for each particle
Is current fitness value better than pBest?
yes
no
Assign current fitness as new pBest
Keep previous pBest
Assign best particle's pBest value to gBest
Calculate velocity for each particle
Use each particle's velocity value to update its data values
Target or maximum epochs reached ?
no
yes
End

Fig. 2 Flowchart of the PSO algorithm

Real-world problems that may take a long time to solve are generally the subject of this type of analysis. An energy optimization problem in a WSN may be solved using a G.A. as follows:

Step 1. An efficient coding of the chromosome occurs in the early stages of development.

Step 2. The person with the greatest fitness function value is selected for the next generation to increase the network's lifespan.

Step 3. Selection produces a mating pool comprised of high-quality individuals.

Step 4. In order to generate new life, two parents are chosen from a large group of deserving candidates. It is reasonable to assume that the new generation's progeny will be more physically fit than their parents.

Step 5. Mutation is also used during the crossover to ensure that the offspring are diverse.

3.2. Proposed Protocol

The proposed minimal energy (MINEN) routing protocol is illustrated in figure 3. As a quick overview, below are the main phases in the procedure:

- Run a sleep schedule to identify nodes not participating in the current epoch. The usage of a sleep schedule is not required to evaluate the protocol's performance; hence this step is optional.
- Formation of clusters and the selection of the cluster head.
- Incorporating edge weights into the DAG construction and connection of all cluster heads.
- For the present period, running Dijkstra to find the cheapest route to the base station.

The assumptions made by the protocol are:

- Initially, all gadgets have equal amounts of power.
- At the Internet of Things, only one base station is permanently installed in a single location.
- An unlimited energy supply means a base station will never go down owing to a lack of energy supply.
- If new cluster heads are elected, and messages can be successfully transmitted from all cluster heads to the base station, we say that a communication cycle has ended.

In the following subsections, we will go through each step of the method presented in Figure 3:

3.2.1. Sleep Scheduling

To save energy, devices that are not in use can be identified using sleep scheduling and turned off at the beginning of each communication round. This article uses GSO, a mixture of PSO and G.A., for sleep schedules. The following is a typical progression for evolutionary optimization approaches:

1. Begin with a population of solutions that are randomly generated.
2. Each solution should be given a fitness score. This fitness rating must reflect the degree to which the existing solution comes near the ideal one.
3. Recovery and re-design of the population of solutions based on their fitness ratings.
4. Repeating step 2 until the perfect solution's conditions have been fulfilled.

A boolean array with the number of nodes in the network as its first element is commonly used as a solution. Each array index has a boolean value that indicates whether or not the device located at that index ought to be put to sleep (true) and whether or not it should (false). A population of solutions is a collection of such arrays. Initially, this population is generated randomly and subjected to a series of operator changes until the desired outcome is reached. It is this population of solutions that distinguishes PSO from G.A.

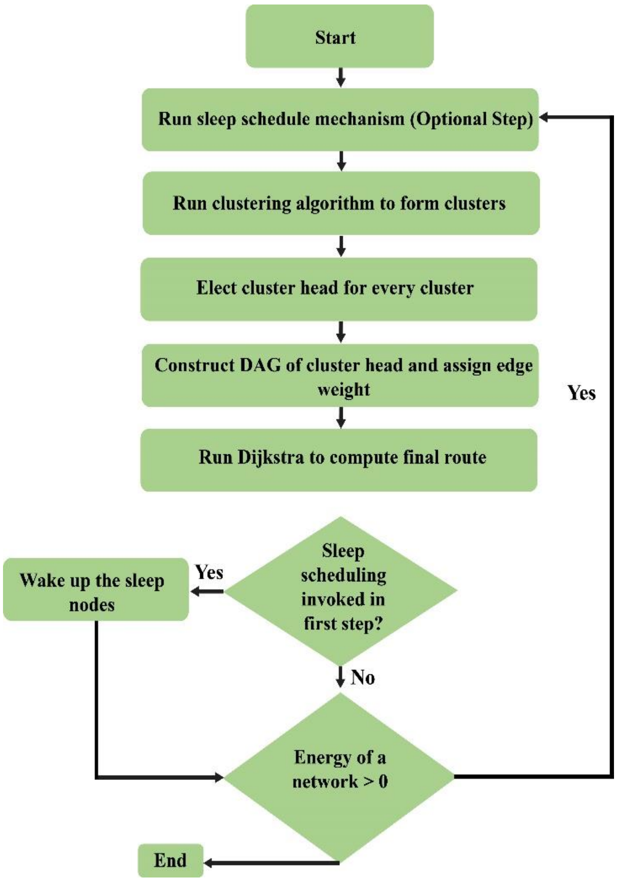
Start
Run sleep schedule mechanism (Optional Step)
Run clustering algorithm to form clusters
Elect cluster head for every cluster
Construct DAG of cluster head and assign edge weight
Run Dijkstra to compute final route
Yes
Sleep scheduling invoked in first step?
Yes
Wake up the sleep nodes
No
Energy of a network > 0
End

Fig. 3 Flow diagram of the algorithm

3.2.2. Cluster Head Election

A head is elected for each cluster following the establishment of clusters. Each device in the cluster has a single point of contact, the cluster head, who is in charge of collecting and transmitting messages to the base station. Because of this, cluster heads are responsible for processing and energy consumption, as well as forming the routing paths that will be addressed later. The problem is that this causes cluster heads to run out of energy relatively quickly. MINEN re-elects the cluster head after a round to prevent the cluster heads from becoming unusable due to battery drain. Cluster leaders are elected for each round based on the remaining battery capacity. The cluster head is the device having the most remaining energy in a given cluster. For example, a rotation of cluster heads results in a more equitable allocation of network resources, extending network life. Cluster heads are picked randomly in this round because all devices have the same amount of energy in the first round.

All of the cluster heads are connected via a Directed Acyclic Graph (DAG) when they are elected. For this DAG, we first set down the energy model we use to estimate the amount of energy used by network devices.

3.2.3. Energy Model

An IoT network's devices must be aware of each other's energy consumption. As a message is transmitted and received, it uses energy. The energy model's energy equations are derived using the following set of variable definitions.

- $E_{r(ij)}$ - transmission of information between devices I and j.
- $E_{t(ij)}$ - The amount of power used to send messages between devices I and j during transmission.
- d_{ij} - the distance between i and j devices.
- d_o - threshold distance
- l_{ij} - the duration of a message transmitted between devices i and j.
- E_{elec} - the energy required for the transmitter or receiver to function.
- ϵ_{MP} - evaluating a multi-path fading channel's energy dissipation.
- $\epsilon_{F\ S}$ - taking into account an open space channel with a direct line of sight.
- R_{ij} - transmission speed between devices i and j.
- $e_{r(ij)}$ - per unit duration of message receipt between devices I and j, message reception energy.
- $e_{t(ij)}$ - per unit time, the message transmission energy between devices i and j are measured.
- e_i - device i current power consumption.
- e_j - device j current energy consumption.
- I - the starting energy value for all gadgets.
- $E_{sf(ij)}$ - The gadgets I and j have used a considerable amount of energy up to this point.

- w_1, w_2, w_3 - edge weight components are allocated weights.

According to the Friis free space model [31] we have,

$$E_{t(ij)} = (E_{elec} + \epsilon_{F\,S}.d^2).l_{ij} \quad \text{for } d_{ij} < d_o \tag{1}$$

$$E_{t(ij)} = (E_{elec} + \epsilon_{MP}\,.d^4).l_{ij} \quad \text{for } d_{ij} \geq d_o \tag{2}$$

$$Er(ij) = Eelec.lij \tag{3}$$

After a certain threshold distance, transmission energy's dependency on distance d_o rise by a factor of two. When two devices, i and j communicate, the data transfer length per unit time (t) is the data transmission rate.

Hence,

$$R_{ij} = l_{ij}/t \tag{4}$$

Equations of energy for message transmission and reception per unit time between devices i and j may be stated as follows using equation 4:

$$e_{t(ij)} = (E_{elec} + \epsilon_{F\,S}.d^2\,).R_{ij} \quad \text{for } d_{ij} < d_o \tag{5}$$

$$e_{t(ij)} = (E_{elec} + \epsilon_{MP}\,.d^4\,).R_{ij} \quad \text{for } d_{ij}\ >= d_o \tag{6}$$

$$er(ij) = Eelec.Rij \tag{7}$$

3.2.4. Flow of the Algorithm

GSO (or MINEN) using Algorithm 2 summarizes the phases of the proposed protocol. If necessary, the sleep scheduling algorithm is executed in the first step of this process. In the second step, the network is organized into clusters. For each network's cluster, devices with the highest residual energy are selected from steps 3 to 7. Using Dijkstra's technique, the minimal cost routing path is determined in steps 8 and 9 by constructing a DAG that connects all cluster heads. Steps 11 and 12 help wake up the required nodes at the end of every round if sleep scheduling was used initially.

4. Simulation and Results

This section discusses the findings of the simulations used to demonstrate the suggested regimen's efficacy. We ran our simulations on the simulator included with [32]. For comparison purposes, we simulated MINEN, LEACH, and FCM:

- The number of active nodes: This assessment tracks the number of nodes engaging in the communication process. If more active devices were connected to the network, its productive capacity would increase proportionally.
- The number of rounds for which a network's energy lasts has been calculated using a comparison of energy vs the number of rounds (time).
- An analysis of the network's geographic coverage over time is done using this method.

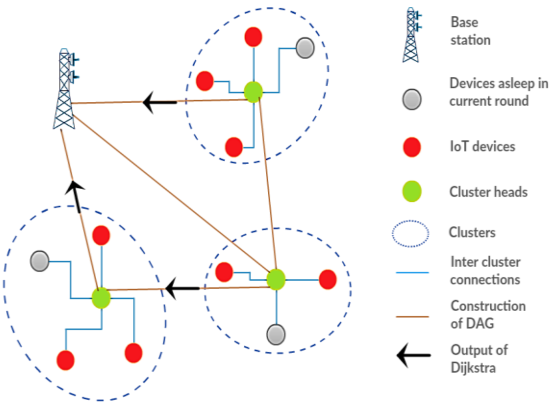

Fig. 4 Sample IoT network with MINEN routing.

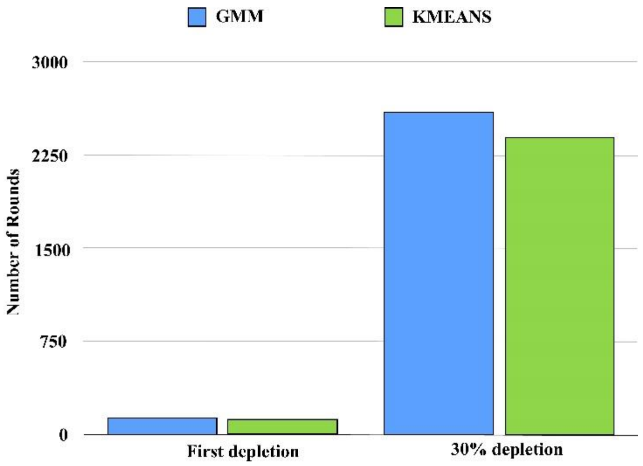

Fig. 5 Clustering algorithms comparison

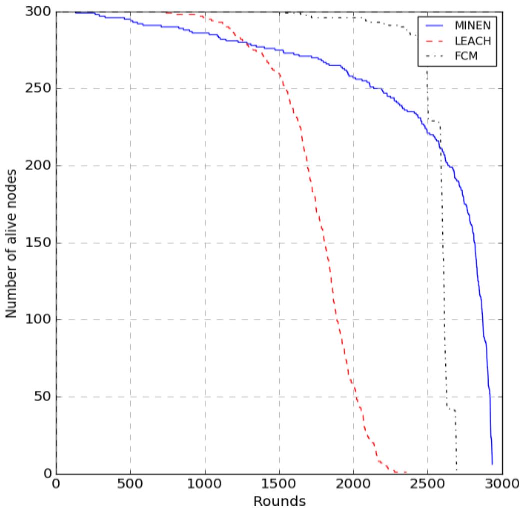

Fig. 6 A graph depicting the IoT network's active nodes.

IoT network nodes' life spans are shown against the number of communication rounds (time) in the simulation in Figure 6. According to the graph, MINEN can maintain 150 devices running for up to 2800 rounds in a network of 300 devices. 150 devices can only be active for 1700 and 2600 rounds using LEACH and FCM, respectively. MINEN has a greater impact on network application operational time than LEACH provides.

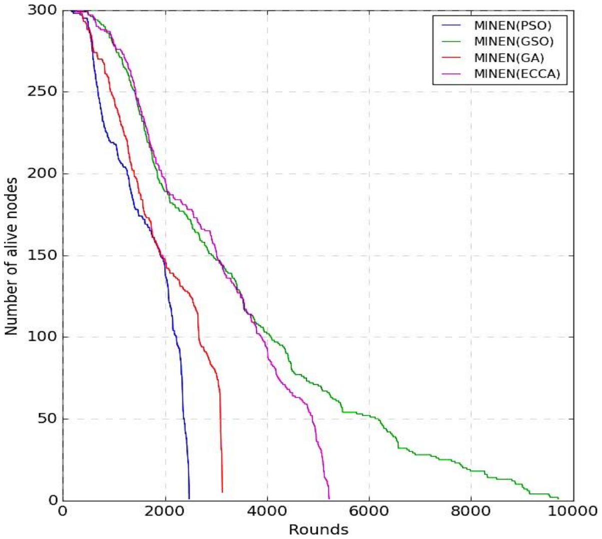

Fig. 7 Represents the IoT network's energy dynamics.

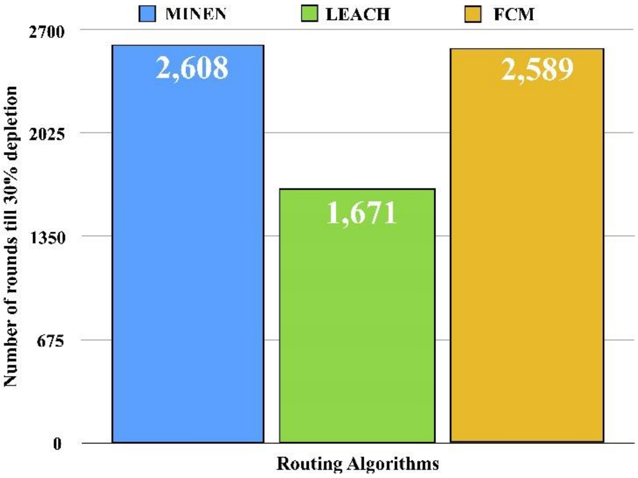

Fig. 8 Number of rounds until 30% of the devices in the network run out of power and stop working.

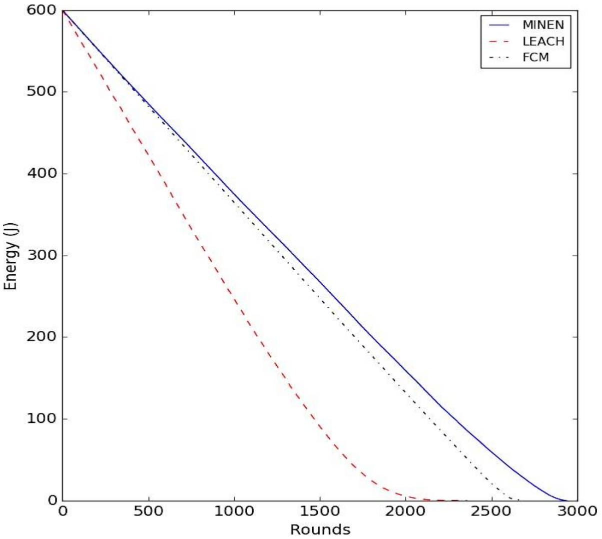

Fig. 9 Plots the network's energy in relation to the number of communication rounds

The IoT network's energy dynamics are depicted. Figure 7 displays the IoT network's energy dynamics. When all of the devices in the network run out of power, the network's energy consumption drops to zero. This occurs after around 3000 rounds of operation for MINEN, 2100 rounds for LEACH, and 2600 rounds for FCM, respectively. The graphs show that LEACH has the greatest energy depletion rate, followed by FCM and MINEN.

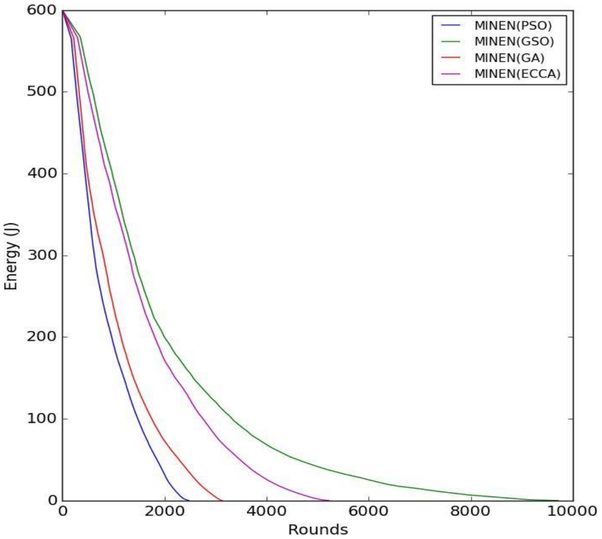

Fig. 10 Displays the number of active nodes in the network in relation to the number of communication rounds

Figure 6 depicts the number of cycles after which 30% of the network's devices run out of energy and become unusable. After approximately 2608 rounds, MINEN reaches 30% depletion. The corresponding numbers are 1671 for LEACH and 2589 for FCM. There is no doubt that MINEN outperforms LEACH and FCM in terms of energy efficiency in Figures 6, 7 and 8. Better cluster head selection criteria and the addition of energy load balancing across multiple communication channels in MINEN are responsible for this performance improvement. We've gone through each of these topics in depth in the preceding sections.

GSO and MINEN are compared to different sleep scheduling algorithms to determine how successful GSO is when used with MINEN. EECA, EECA, and PSO are the sleep scheduling algorithms that have been tested. The number of active nodes and the network's energy dynamics is used to assess these techniques. Figure 9 depicts the network's energy as a function of the number of communication cycles it has been through. The chart shows that MINEN and GSO can keep the network running for about 10,000 rounds of communication. The devices in the network are kept active for about 6000 rounds by MINEN with EECA, 3000 rounds by G.A., and 2500 rounds by PSO instead. There are no significant differences in terms of slopes between GSO and the other algorithms in terms of energy consumption per round (time). PSO depletes energy the fastest, whereas GSO depletes energy the least. It is shown in Figure 10 that the number of nodes that are still alive is proportional to the number of communications. It confirms what we saw in Figure 9 and shows that MINEN, when combined with GSO, outperforms all other current sleep scheduling methods.

5. Conclusion and Future scope

This study proposes a routing system for IoT-WSNs that consumes the least amount of energy. In order to minimize the overall cost of energy consumption, MINEN uses a clustering method to distribute it equally among all of the network's nodes. Clustering, cluster head rotation, energy reduction across connections, and low-residual-energy assisting devices are used to accomplish this. This is done by creating a DAG with the cluster heads as the graph nodes. A cost/weight is then allocated to the edges based on the energy used to send and receive messages across a specific connection and a factor called energy spent thus far, which refers to the device pair that forms a communication link (Esf). The Esf factor ensures that the application's load is evenly distributed over all its connections based on energy consumption.

In order to determine the shortest (and hence least energy-intensive) route for sending messages from the sender cluster head to the base station, Djikstra's technique is then used. The energy-saving efforts are further bolstered by adding the Genetic Swarm Optimization (GSO) sleep scheduling method to MINEN. Supplementing MINEN with GSO improves its performance over other methods of sleep schedule. While LEACH and FCM are popular energy-efficient routing protocols that have been around for a while, MINEN is the only one that surpasses both of them.

It is possible to extend the protocol to networks where all IoT nodes are mobile, and there are no direct links between the source and destination nodes. Furthermore, there is room for improvement in the sleep scheduling algorithms used in the article. Additionally, it may be worthwhile to investigate alternate clustering methods that might provide better clusters and hence higher energy conservation.

References

[1] Sadrishojaei M, Jafari Navimipour N, Reshadi M, et al., “An Energy-Aware Clustering Method in the Iot Using a Swarm-Based Algorithm,” *Wireless Network*, vol. 28, pp. 125–136, 2022. Crossref, https://doi.org/10.1007/s11276-021-02804-x

[2] Xiao N, et al., “A Diversity-Based Selfish Node Detection Algorithm for Socially Aware Networking,” *Journal of Signal Processing Systems*, vol. 93, pp. 811–825, 2021.

[3] Lv Z, Qiao L, Li J, & Song H, “Deep-Learning-Enabled Security Issues in the Internet of Things,” *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9531–9538, 2020. Crossref, https://doi.org/10.1109/JIOT.2020.3007130

[4] Lv Z, Lou R, Li J, Singh A. K, & Song H, “Big Data Analytics for 6G-Enabled Massive Internet of Things,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5350–5359, 2021. Crossref, https://doi.org/10.1109/JIOT.2021.3056128

[5] Sohaib A. Latif, Fang B. Xian Wen, Celestine Iwendi, Li-li F. Wang, Syed Muhammad Mohsin, Zhaoyang Han, and Shahab S. Band, “AI-Empowered, Blockchain and SDN Integrated Security Architecture for Iot Network of Cyber Physical Systems,” *Computer Communications*, vol. 181, pp. 274-283, 2022. Crossref, https://doi.org/10.1016/j.comcom.2021.09.029

[6] J. Agarkhed, V. Kadrolli and S.R. Patil, “Efficient Bandwidth-Aware Routing Protocol in Wireless Sensor Networks (EBARP),” *International Journal of Information Technology*, vol. 14, pp. 1967–1979, 2022. Crossref, https://doi.org/10.1007/s41870-021-00828-2

[7] Z. Yiming, L. Mandan and L. Qingwei, “An Energy Balanced Clustering Protocol Based on an Improved CFSFDP Algorithm for Wireless Sensor Networks,” *Sensors*, vol. 18, no. 3, pp. 881, 2018. Crossref, https://doi.org/10.3390/s18030881

[8] A. A. Baradaran and K. Navi, “HQCA WSN: High Quality Clustering Algorithm and Optimal Cluster Head Selection Using Fuzzy Logic in Wireless Sensor Networks,” *Fuzzy Sets and System*, vol. 389, pp. 114-144, 2020. Crossref, https://doi.org/10.1016/j.fss.2019.11.015

[9] X. Yuan, M. Elhoseny, H. K. El Minir and A. M. Riad, “A Genetic Algorithm Based Dynamic Clustering Method Towards Improved WSN Longevity,” *Journal of Network and Systems Management*, vol. 25, pp. 21-46, 2017. Crossref, https://doi.org/10.1007/s10922-016-9379-7

[10] M. O. Oladimeji, M. Turkey and S. Dudley, “HACH: Heuristic Algorithm for Clustering Hierarchy Protocol in Wireless Sensor Networks,” *Applied Soft Computing*, vol. 55, pp. 452-461, 2017. Crossref, https://doi.org/10.1016/j.asoc.2017.02.016

[11] B. Singh and D. K. Lobiyal, “Energy Preserving Sleep Scheduling for Cluster-Based Wireless Sensor Networks,” *2013 Sixth International Conference Contemporary Computing (IC3)*, Noida, India, pp. 97–101, 2013. Crossref, https://doi.org/10.1109/IC3.2013.6612169

[12] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. MeliaSegui, and T. Watteyne, "Understanding the Limits of Lorawan," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34-40, 2017. Crossref, https://doi.org/10.1109/MCOM.2017.1600613

[13] LoRa Alliance, “LoRaWAN Specification V1.1,” *LoRa Alliance*, 2017.

[14] B. Reynders, W. Meert, and S. Pollin, “Power and Spreading Factor Control in Low Power Wide Area Networks,” *IEEE ICC 2017 SAC Symposium Internet of Things Track (ICC'17 SAC-7 IoT)*, pp. 1-5, 2017. Crossref, https://doi.org/10.1109/ICC.2017.7996380

[15] Kh. Abdelfadeel, V. Cionca and D. Pesch, “Fair Adaptive Data Rate Allocation and Power Control in LoRaWAN," *IEEE 19th International Symposium on A World of Wireless, Mobile and Multimedia Networks,* 2018. Crossref, https://doi.org/10.1109/WoWMoM.2018.8449737

[16] V. Hauser and T. Hgr, “Proposal of Adaptive Data Rate Algorithm for Lorawan-Based Infrastructure,” *IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud),* pp. 85-90, 2017. Crossref, https://doi.org/10.1109/FiCloud.2017.47

[17] M. Slabicki, G. Premsankar, and M. D. Francesco, “Adaptive Configuration of Lora Networks for Dense Iot Deployments,” *IEEE/IFIP Network Operations and Management Symposium,* 2018. Crossref, https://doi.org/10.1109/NOMS.2018.8406255

[18] C. Srinivasan, B. Rajesh, P. Saikalyan, K. Premsagar and ES. Yadav, “A Review on the Different Types of Internet of Things (IoT),” *Journal of Advanced Research in Dynamical and Control Systems,* vol. 11, no. 1, pp. 154-158, 2019.

[19] MA. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (Iot) Security,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, 2020. Crossref, https://doi.org/10.1109/COMST.2020.2988293

[20] K. Haseeb, N. Islam, T. Saba, A. Rehman and Z. Mehmood, “LSDAR: A Lightweight Structure based Data Aggregation Routing Protocol with Secure Internet of Things Integrated Next-Generation Sensor Networks,” *Sustainable Cities and Society,* vol. 54, pp. 101995, 2020. Crossref, https://doi.org/10.1016/j.scs.2019.101995

[21] S. Vadivelu and P. Suresh Babu, “Survival Study on Energy and Bandwidth Efficient Data Transmission in Wireless Networks,” *SSRG International Journal of Computer Science and Engineering,* vol. 9, no. 8, pp. 1-6, 2022. Crossref, https://doi.org/10.14445/23488387/IJCSE-V9I8P101

[22] K. Haseeb, N. Islam, A. Almogren and Din IU, “Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things,” *IEEE Access,* vol. 7, pp. 185496-185505, 2019. Crossref, https://doi.org/10.1109/ACCESS.2019.2960633

[23] G. Prabaharan and S. Jayashri, “Mobile Cluster Head Selection Using Soft Computing Technique in Wireless Sensor Network,” *Soft Computing,* vol. 23, no. 1, pp. 8525-8238, 2019. Crossref, https://doi.org/10.1007/s00500-019-04133-w

[24] F. Zawaideh and M. Salamah, “An Efficient Weighted Trust-Based Malicious Node Detection Scheme for Wireless Sensor Networks,” *International Journal of Communication Systems,* vol. 32, no. 3, pp. e3878, 2019. Crossref, https://doi.org/10.1002/dac.3878

[25] K. Haseeb, A. Almogren, N. Islam, I. Ud Din and Z. Jan, “An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in Iot-Based WSN,” *Energies,* vol. 12, no. 21, pp. 4174, 2019. Crossref, https://doi.org/10.3390/en12214174

[26] W. She, Q. Liu, Z. Tian, J-S. Chen, B. Wang and W. Liu, “Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks,” *IEEE Access*, vol. 7, pp. 38947-38956, 2019. Crossref, https://doi.org/10.1109/ACCESS.2019.2902811

[27] M. Jamshidi, SSA. Poor, A. Arghavani, M. Esnaashari, AA. Shaltooki and MR. Meybodi, “A Simple, Lightweight, and Precise Algorithm to Defend Against Replica Node Attacks in Mobile Wireless Networks Using Neighboring Information,” *Ad Hoc Networks,* vol. 100, pp. 102081, 2020. Crossref, https://doi.org/10.1016/j.adhoc.2020.102081

[28] NA. Khalid, Q. Bai and A. Al-Anbuky, “Adaptive Trust-Based Routing Protocol for Large Scale WSNs,” *IEEE Access,* vol. 7, pp. 143539–143549, 2019. Crossref, https://doi.org/10.1109/ACCESS.2019.2944648

[29] LB. Oliveira LB, A. Ferreira, MA. Vilaça, HC. Wong, M. Bern, R. Dahab and AA. Loureiro, “SecLEACH—on the Security of Clustered Sensor Networks,” *Signal Processing,* vol. 87, no. 12, pp. 2882-2895, 2007. Crossref, https://doi.org/10.1016/j.sigpro.2007.05.016

[30] SH. Alsamhi, O. Ma, MS. Ansari and Q. Meng, “Greening Internet of Things for Greener and Smarter Cities: A Survey and Future Prospects,” *Telecommunication Systems,* vol. 72, pp. 609-632, 2019. Crossref, https://doi.org/10.1007/s11235-019-00597-1

[31] V. Subbarao, K. Srinivas and R. Pavithr, “A Survey on Internet of Things Based Smart, Digital Green and Intelligent Campus,” *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE,* 2019. Crossref, https://doi.org/10.1109/IoT-SIU.2019.8777476

[32] K. Latif, A. Ahmad, N. Javaid, ZA. Khan and N. Alrajeh, “Divide-and-Rule Scheme for Energy Efficient Routing in Wireless Sensor Networks,” *Procedia Computer Science,* vol. 19, pp. 340-347, 2013. Crossref, https://doi.org/10.1016/j.procs.2013.06.047

[33] V. Saranya, S. Shankar and G. Kanagachidambaresan, “Energy Efficient Clustering Scheme (EECS) for Wireless Sensor Network With Mobile Sink,” *Wireless Personal Communications,* vol. 100, pp. 1553-1567, 2018. Crossref, https://doi.org/10.1007/s11277-018-5653-1

[34] V. Saranya, S. Shankar and G. Kanagachidambaresan, “Energy Efficient Data Collection Algorithm for Mobile Wireless Sensor Network,” *Wireless Personal Communications*, vol. 105, pp. 219-232, 2019. Crossref, https://doi.org/10.1007/s11277-018-6109-3

[35] T. Wang, G. Zhang, A. Liu, MZA. Bhuiyan and Q. Jin, “A Secure Iot Service Architecture with an Efficient Balance Dynamic Based on Cloud and Edge Computing,” *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 4831-4843, 2019. Crossref, https://doi.org/10.1109/JIOT.2018.2870288

[36] A. Yousefpour, A. Patil, G. Ishigaki, I. Kim, X. Wang, HC. Cankaya, Q. Zhang, W. Xie and JP. Jue, “FogPlan: A Lightweight Qos-Aware Dynamic Fog Service Provisioning Framework,” *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 5080-5096, 2019. Crossref, https://doi.org/10.1109/JIOT.2019.2896311

[37] B. Kim and J. Song, “Energy-Efficient and Secure Mobile Node Reauthentication Scheme for Mobile Wireless Sensor Networks,” *EURASIP Journal on Wireless Communications and Networking*, pp. 155, 2019. Crossref, https://doi.org/10.1186/s13638-019-1470-9

[38] J. Tan, W. Liu, T. Wang, NN. Xiong, H. Song, A. Liu and Z. Zeng, “An Adaptive Collection Scheme-Based Matrix Completion for Data Gathering in Energy-Harvesting Wireless Sensor Networks,” *IEEE Access,* vol. 7, pp. 6703-6723, 2019. Crossref, https://doi.org/10.1109/ACCESS.2019.2890862

[39] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy and A. Kannan, "Energy Aware Cluster and Neuro-Fuzzy Based Routing Algorithm for Wireless Sensor Networks in IoT," *Computer Networks,* vol. 151, pp. 211-223, 2019. https://doi.org/10.1016/j.comnet.2019.01.024

[40] M. Elhoseny and AE. Hassanien, "Expand Mobile WSN Coverage in Harsh Environments, in "*Dynamic Wireless Sensor Networks, Springer,* pp. 29-52, 2019. https://doi.org/10.1007/978-3-319-92807-4_2