SN Computer Science (2024) 5:546
https://doi.org/10.1007/s42979-024-02778-5

ORIGINAL RESEARCH

Artificial Intelligence in Next-Generation Networking: Energy Efficiency Optimization in IoT Networks Using Hybrid LEACH Protocol

Surbhi Bhatia Khan[1] · Ankit Kumar[2] · Arwa Mashat[3] · Dayananda Pruthviraja[4] · Mohammad Khalid Imam Rahmani[5] · Jimson Mathew[6]

Received: 30 October 2023 / Accepted: 27 January 2024

Abstract
The convergence of the Internet of Things (IoT) and Artificial Intelligence (AI) is significantly transforming the landscape of future networking. The Internet of Things (IoT) is a technological paradigm that encompasses embedded systems, wireless sensors, and automation, facilitating the integration of various applications ranging from smart homes to wearable devices. In addition, the advent of artificial intelligence (AI) amplifies this influence by providing data-driven analytics, optimising processes, and presenting novel opportunities for growth. Nevertheless, the widespread adoption of devices within Internet of Things (IoT) networks gives rise to apprehensions regarding increased energy consumption. In order to ensure the longevity of network operations, it is imperative to employ energy-efficient protocols for sensor nodes that possess limited power resources. One example of a protocol that demonstrates this concept is the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol. This protocol effectively divides networks into clusters and dynamically adjusts the cluster heads to optimise the transmission of data to the base stations. Our study enhances the LEACH protocol by incorporating digital twin simulation, thereby enhancing the efficiency of IoT systems. Virtual network models and AI analytics are employed to assess energy consumption and performance. Cache nodes play a crucial role within this framework as they collect data from cluster heads in order to transmit it to the base station. By leveraging artificial intelligence (AI) and simulation techniques, we are able to improve the energy efficiency and reliability of the Internet of Things (IoT) systems. The findings indicate a significant reduction of 83% in non-functioning nodes and a notable increase of 1.66 times in energy levels of nodes compared to conventional approaches. This study highlights a potential direction for energy-efficient, AI-enhanced Internet of Things (IoT) networking through the utilisation of the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol.

Keywords Internet of things · LEACH · Data aggregation · Clustering · Cluster head · Lifetime · Gateway

Introduction

In the year 2019, a majority of 53% of the population resided in urban areas. According to projections, it is anticipated that by the year 2050, the proportion of the population might potentially reach as high as 70%. Over 10 billion individuals are projected to reside, engage in consumption, and require services within these megacities. The perpetual need for essential resources such as water and electricity, along with the generation of waste and the release of pollutants, has necessitated the urgent reduction and mitigation of the environmental impact caused by these causes. Ensuring the optimal utilisation of these resources over an extended duration is crucial. Ensuring the feasibility of their utilisation for future generations is imperative. It is vital to ensure the perpetual continuation of their utilisation. The global community is currently through a transformative phase characterised by the increasing integration of interconnected machines, which holds the potential to foster a sense of interconnectedness among individuals worldwide. In contemporary society, individuals possess elevated demands for the quality of information and services they get. Simultaneously, companies and governmental institutions have gained access to advanced technological resources, enabling them to provide valuable, streamlined, and impactful sustainable services. Modern technology enables the

This article is part of the topical collection "Artificial Intelligence for Next-generation Edge Networks" guest edited by Mainak Adhikari, Abhishek Hazra and Sudarshan Nandy.

Extended author information available on the last page of the article

Published online: 15 May 2024

ongoing surveillance and control of various aspects, such as air and water quality, public transportation, traffic patterns, weather conditions, and energy production and consumption, by utilising sensor data. A city is considered "smart" when many data sources, such as buildings, autos, industries, power plants, and lighting systems, are interconnected. Machine-to-Machine (M2M) services, which serve as the foundation of intelligent services, are not entirely novel. Indeed, these technologies have been employed across many sectors since the latter part of the 1990s, with particular prominence observed in the commercial and industrial domains. Indeed, it is worth noting that the industrial sector extensively utilises applications of the Internet of Things (IoT) for the specific objectives of monitoring and maintaining facilities (68%), conducting remote operations (54%), and establishing device connectivity through Wi-Fi (70%). The information provided to us has been graciously contributed by Aruba.

These applications are encompassed under the framework of Industry 4.0, often regarded as the fourth industrial revolution. The term "Industry 4.0" encompasses the integration of digital technologies throughout several aspects of the industrial industry. Moreover, the energy consumption inside metropolitan areas of the European Union (EU) constitutes around 60% to 80% of the total energy utilisation. In this particular context, the objective of integrating the Internet of Things (IoT) and enhancing energy efficiency should be to meet the requirements of residents for valuable services, while simultaneously reducing overall energy consumption and enhancing resource utilisation efficiency. Vermesan and Friess [1] suggest that there is an expected rise in the use of Internet of Things (IoT) applications in the future. The Internet of Things (IoT) refers to a network that enables the connection of diverse physical objects, in contrast to conventional internet connections. The product range encompasses a diverse array of items, such as automobiles, smartphones, and household appliances, alongside toys, cameras, and several more things available in various configurations and sizes. The applications of the Internet of Things (IoT) enable people to get internet connectivity and access a diverse range of advanced software and communication services. things has the capability to establish connections among themselves and with additional things, so facilitating access to media and fostering an interconnected world via the Internet of Things (IoT). One notable characteristic of the Internet of Things is the ubiquitous presence of embedded computing devices, often powered by microchips, within every physical object. The uniqueness of the Internet of Things (IoT) is exemplified by this particular element. This particular attribute is what bestows the Internet of Things with its nomenclature. This facilitates the integration of many technologies into the foundational infrastructure of the Internet of Things. Radio frequency identification (RFID), sensors, actuators, miniaturisation, nanotechnology, and smart entities are all technological examples encompassed within this category. The Internet of objects (IoT) may be categorised into three main subsets: (1) communication between people and machines or objects; (2) communication between machines; and (3) communication between individuals. The subcategories encompass interactions facilitated by the internet, as classified by Vermesan and Friess [2].

The interconnected system of commonplace objects is commonly known as the Internet of Things (IoT). The effective utilisation of computational and networking resources has been facilitated by the implementation of the Internet of Things (IoT) in many applications, as discussed by Vermesan et al. [3]. The process of communication in self-configuring wireless networks can be likened to the intricate interweaving of a complicated web, where many connecting elements play a crucial role in establishing and maintaining connectivity. The networks enable the integration of diverse communication capabilities by connecting a range of devices in a communication chain. Radio-Frequency Identification (RFID) is a technology that utilises a Wi-Fi layer integrated with the internet infrastructure to establish worldwide systems of RFID tags. It is a significant component of the Internet of Things (IoT), a concept denoting the interconnectedness of various devices and objects over the internet. Connected objects and computers inside a network have the ability to establish communication with each other. These entities are incorporated into intricate systems and employ diverse sensors to gather data, including temperature and other relevant information, from their immediate surroundings. To meet the requirements of the existing applications, the collected information is sent to nearby sensors for processing. The objectives of this work are given as below:

- To study the indepth literature behind protocols needed to enhance the efficiency of IoT systems including LEACH protocol.
- Minimize energy consumption for data transmission by selecting appropriate cluster heads based on residual energy.
- To balance energy and proximity and Enhance LEACH-C protocol.
- To conduct simulations on the proposed algorithms to demonstrate considerable improvement in energy levels of nodes compared to conventional approaches.

Clustering of Nodes in WSN

The network topology is said to as flat when all sensor nodes are assigned similar duties, which involve the collection and transmission of identical data. Prominent instances of flat routing protocols in the context of Wireless Sensor Networks (WSNs) encompass SPIN [4], directed diffusion [5], and rumour routing [6]. The protocols utilise a data-centric methodology in order to reduce the need for retransmissions. This means that sensor nodes are only required to communicate data that is relevant to the queries or interests that have been propagated by requesters. Nevertheless, as the number of nodes in the network grows, the intricacy of these protocols also rises. Therefore, although flat routing has certain benefits, the management of scalability and mobility becomes complex, especially in resource-limited Wireless Sensor Networks (WSNs) [7] (Fig. 1).

Within hierarchical networks, individual nodes undertake certain functions, with certain nodes being responsible for energy-intensive operations such as data collecting and aggregation, while others are dedicated purely to environmental sensing. One method for assigning unique roles is through the process of dividing the network into clusters or groups. Each cluster consists of a certain group of nodes, in which one node is assigned as the Cluster Head (CH) [8], while the remaining nodes are designated as Cluster Members (CMs). The aforementioned arrangement exhibits a hierarchical structure consisting of three tiers: the lowest layer comprises CMs, the next tier comprises CHs, and the highest tier accommodates a Base Station (BS). The collected data from the CMs is transmitted to the appropriate CHs, which then aggregate or fuse the obtained data prior to transferring it to the BS for further processing. The hierarchical structure of this organisation efficiently distributes duties and enables streamlined data handling inside the network.

Cluster Based Protocols in WSN

Each networking protocol possesses its own set of advantages and disadvantages, making the selection of a specific protocol contingent upon the particular application of the network at hand.

The Low Energy Adaptive Clustering Hierarchy (LEACH) protocol, known as Low Energy: Adaptive Clustering Hierarchy, stands out as a prominently employed cluster-based routing protocol. This protocol's central concept revolves around the cyclic rotation of the cluster head (CH) role among diverse nodes. This mechanism aims to prevent premature node depletion resulting from battery drain. LEACH utilizes a distributed algorithm to facilitate the creation of clusters, wherein nodes autonomously determine whether to assume the role of a cluster head, obviating the need for centralized control. Once cluster heads (CHs) are designated, they serve as leaders for a specific duration termed the "round time." Subsequently, new clusters are formed.

Each round within the LEACH protocol comprises two distinct phases:

i. Set-up Phase: During this phase, cluster formation takes place. ii. Steady-State Phase: This phase is dedicated to actual data transfer.

i. Every node 's' within the network randomly generates a number 'X' within the range of 0 to 1. The generated number 'X' is then juxtaposed with the threshold value 'T(s)'.
ii. If 'X' is found to be less than 'T(s)', the node 's' makes the decision to undertake the role

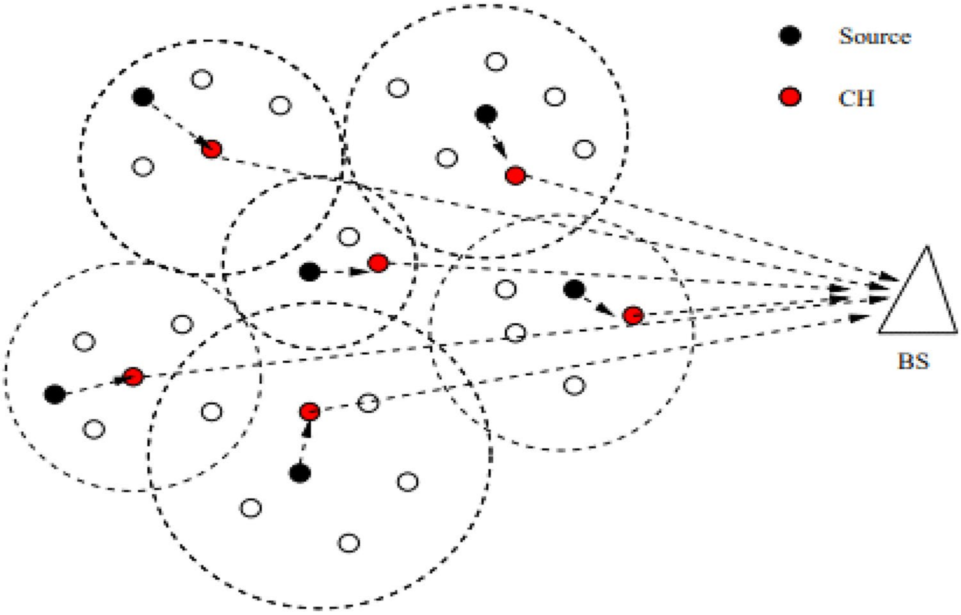


Fig. 1 Basic structure of clustering in WSN

of a cluster head for the ongoing round. The Eq. (1) is given below:

$$T(s) = \begin{cases} \frac{p}{1-p\times\left(r\times1\bmod\frac{1}{p}\right)}, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

The LEACH protocol utilises the variable 'p' to represent the predetermined number of cluster heads, 'r' to denote the present round, and 'G' to signify the set of nodes that have not yet been designated as cluster heads. The primary responsibility of each cluster leader is to initiate the dissemination of an advertising message. The nodes assess the signal strength of these advertisements when making decisions on alignment with cluster leaders. After the formation of clusters, the cluster heads (CHs) generate a TDMA (Time Division Multiple Access) schedule that is tailored to their members and disseminate it among their respective clusters [9]. During the steady-state phase, the nodes engage in data communication with the cluster heads assigned to their respective clusters at the designated time intervals. Following the termination of a Time Division Multiple Access (TDMA) frame, the cluster head will proceed to consolidate or merge the received data and subsequently compile it into a unified set prior to transmitting it to the base station. The LEACH protocol incorporates the Code Division Multiple Access (CDMA) principle to mitigate intra-cluster interference. Each cluster head possesses an own and specific code, which it used to transmit its data to the other nodes within the cluster. Following the completion of the round period, the network will undergo a further transition into the forthcoming set-up phase. This phase will involve the network being tasked with the generation of supplementary clusters. When compared to alternative clustering approaches, dynamic clustering has been found to be more successful in terms of preserving the energy resources of the network. Although LEACH [10] has several advantages, it nevertheless faces several challenges. One concern arises from the possibility that nodes with less resources may be selected as cluster leaders, leading to a higher energy consumption rate. Furthermore, the decentralised nature of cluster creation places additional strain on the sensor nodes.

In a concise manner, the operational architecture of LEACH encompasses a diverse range of processes, including cluster head selection, data transmission and aggregation, as well as interference management and energy conservation. While the protocol presents a flexible and responsive approach to clustering in wireless sensor networks, it is crucial to acknowledge and mitigate the possible limitations [12]. These limitations include the suboptimal choice of cluster heads and the heightened resource requirements imposed on individual sensor nodes during the cluster formation procedure (Fig. 2).

LEACH is the basis for a great many different clustered protocols that have been devised for wireless sensor networks and acts as their inspiration. A wide variety of modified iterations based on LEACH have arisen within the current body of research. These iterations include designs such as LEACH-C [13], E-LEACH [14], MR-LEACH [15], VLEACH [16], LEACH-FL [17], W-LEACH [18], and T-LEACH [19], amongst others.

When compared to LEACH, the Power-Efficient Gathering in Sensor Information Systems (LEACH) [20] protocol stands out as an improved version of the latter. Within the scope of this discussion, a proactive and greedy method is used to form a sequential chain of nodes. Each individual node that makes up this chain takes up the function of data receiver from the node that came before it in the chain. After then, the node adds its own data to the dataset that it has received, aggregates the information that has been gathered, and then sends the combined data on to the node that comes next in the chain. This pattern of actions involving the processing of data continues until the data are successfully sent to the base station (BS) [21].

The following steps are taken in the procedure, which are represented in Fig. 3:

1. The information collected by Node A is sent on to Node B.
2. The data that Node B obtained from Node A is combined with the data that it has previously collected.
3. The data that has been aggregated is sent to Node D via Node E.

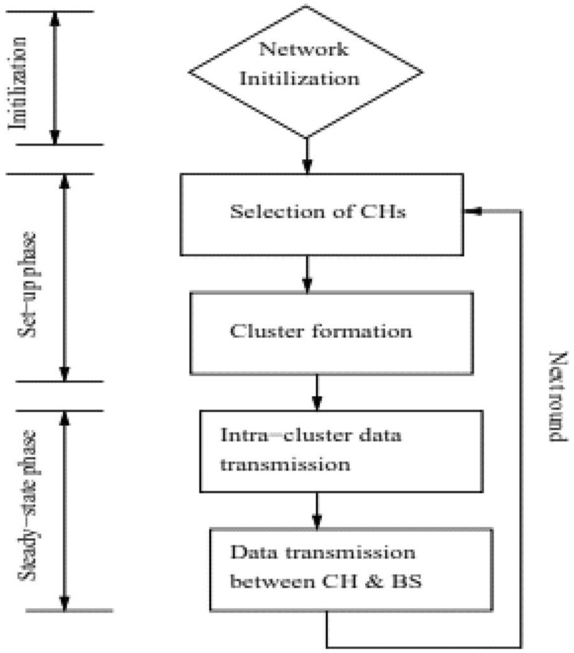


Fig. 2 A graphical representation of the LEACH process

4. The aggregation procedure is performed again by Node D, which combines the newly received data with the data it already has.

After some time, Node C, which is in the position of the leader, will eventually take data from both of its neighboring nodes, which are Node D and Node E. It will then blend these datasets before sending the combined information to the base station.

This protocol architecture, which is represented in Fig. 3, shows the collaborative data aggregation technique that LEACH [22] employs. This mechanism highlights LEACH's potential to promote efficient and energy-saving data collection inside sensor networks.

In the unfortunate event that one of the nodes in the network fails, there will be a requirement inside the network to rebuild the chain. An intriguing mechanism is brought into play by the LEACH protocol. The data aggregation process is carried out at each node along the chain, with the exception of the leader node, which is located in the position closest to the base station (BS). A single node, which is referred to as the designated leader node in LEACH, is given the task of relaying the aggregated data to the BS in LEACH, which is a divergence from the method that LEACH takes [23], which is characterized by having several cluster heads. Because the challenging activity of long-distance transmission is centralized inside a single node, this one-of-a-kind structure improves the energy efficiency of the system. Although LEACH is a method of transmission that makes effective use of energy, it does result in a noticeable delay for the data as it travels through the nodes on its way to the BS. This data propagation across each link in the chain results in the introduction of a delay factor, which in turn has an effect on the performance of the network as a whole. Hierarchical-LEACH, often known as H-LEACH, is a novel iteration of LEACH that was developed to solve the problem of excessive latency. When H-LEACH was being developed, one of its primary focuses was on finding ways to reduce the amount of time lost during the process of sending packets to the BS. The clever improvement that was brought about by H-LEACH takes advantage of the spatial separation of nodes and uses it to its advantage. This architecture allows for physically dispersed nodes to participate in parallel data transmissions, which is an approach that significantly reduces the latency that is often associated with traditional sequential transmission. The use of Code Division Multiple Access (CDMA) coding has been included into H-LEACH in order to eliminate the possibility of signal interference, which might slow down simultaneous data transmission. This sophisticated method guarantees that concurrent transmissions go without hiccups and in an undisturbed manner. In spite of the encouraging advancements that have been brought about by both LEACH and H-LEACH, there is a significant feature that deserves notice. Neither protocol takes into account the essential factor of energy expenditure during the process of chain building. Because of this, both LEACH and its improved counterpart, H-LEACH, call for extra overhead in order to change the dynamic topology of the sensor network so that it can consider the different energy situations. This requirement highlights the continued difficulty of finding a harmonic balance between the optimization of network performance and the efficiency of energy use in the network.

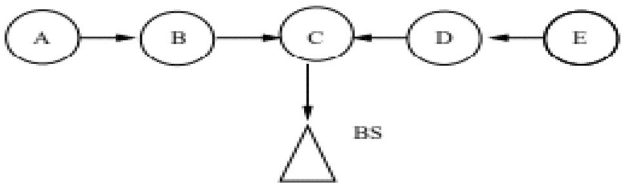


Fig. 3 Displays the sequential collection of data by nodes inside LEACH

IoT and Related Future Technologies

Various subsystems and objects that operate within a unified platform are connected using communication and IT technologies, which are integrated with wired and wireless control systems. The Internet of Things (IoT) has emerged as a game-changing technology, allowing the integration of numerous physical items and systems and opening the way for smart cities, smart homes, intelligent transportation systems, healthcare improvements, and industrial automation. IoT applications have seen greater capabilities and better performance with the introduction of digital twin technology, which produces virtual clones of actual assets. This article delves into current research on IoT and related future technologies, with a particular emphasis on the incorporation of digital twins [24].

Exploring the possibilities of IoT-enabled applications linked with digital twin technology is one of the important areas of study in this subject. Smart cities, for example, use IoT and digital twin to monitor and control vital infrastructure, maximize resource use, and improve urban livability. Building transportation and utility, digital twins provide real-time monitoring, predictive maintenance, and optimal resource allocation. Similar applications may be seen in the smart home arena, where digital twins of residential structures and equipment offer customized automation, energy management, and improved occupant comfort. Another sector where the combination of IoT and digital twins is making major gains is healthcare. Patients' and medical equipment's digital twins enable remote monitoring, individualized therapy, and predictive analysis, resulting in better healthcare results [25].

In addition to investigating IoT applications with digital twins, research is focusing on developing future technologies that will support this ecosystem synergistically. Edge computing, for example, is critical in IoT applications [26] because it allows for real-time data processing and analytics at the network edge. This reduces latency, improves data security, and maximizes bandwidth consumption. 5G networks are expected to transform IoT deployments by allowing enormous device connections and supporting mission-critical applications with high-speed, low-latency communication [27]. To allow intelligent decision-making, anomaly detection, and predictive analytics, artificial intelligence (AI) and machine learning algorithms are being linked to IoT and Digital twin. These technologies enable digital twins to learn and adapt to real-time data, allowing them to simulate actual assets more accurately and efficiently. Blockchain technology ensures trust and integrity in data exchange and communication in IoT contexts by enabling safe and transparent transactions. Cloud computing systems provide a scalable infrastructure for handling and analyzing massive volumes of IoT data, allowing for data-driven insights and promoting cooperation among many stakeholders [28].

Simulations of digital twins have also emerged as an important technique for enhancing IoT systems. Digital twins allow testing, monitoring, and predictive analysis of IoT systems by constructing virtual counterparts of actual assets. Before adopting IoT solutions in the actual world, organizations may simulate various situations, assess performance, detect possible difficulties, and optimize resource allocation. This decreases costs, eliminates risks, and allows for more effective decision-making. In the industrial industry, for example, digital twins of production lines may be used to simulate and improve production processes, increasing efficiency and reducing downtime. Digital twin simulations in transportation may help with traffic management, route optimization, and congestion reduction. Digital twins in energy systems can mimic and optimize the use of renewable resources, enhancing efficiency and sustainability.

While investigating the possibilities of IoT and digital twins, it is critical to address cybersecurity and privacy concerns. Because IoT networks entail a great deal of data exchange and communication, strong security measures are required to guard against cyber-attacks. For IoT and digital twin contexts, recent research has concentrated on establishing secure communication protocols, encryption approaches, access control mechanisms, and privacy-preserving algorithms. Maintaining confidence and dependability in these systems requires ensuring data integrity, confidentiality, and availability.

Finally, new research on IoT and similar future technologies with digital twin [29] integration shows the enormous potential of this combination. The synergy between IoT and digital twin is altering the way we interact with the physical world, from allowing breakthrough applications in smart cities, smart homes, healthcare, and industrial automation to developing technologies like edge computing, 5G networks, AI, and blockchain.

Components of IoT

The Internet of Things (IoT) is an essential part of digital twin technology because it paves the way for the gathering and transfer of real-time data from the actual products or systems that are being modelled. This makes the IoT an essential part of digital twin technology.

RFID, which stands for radio frequency identification, is an essential part of the Internet of Things environment. It entails the use of RFID tags, in addition to the establishment of a worldwide infrastructure to support these tags. On top of the internet is a wireless layer, which enables computers and other linked devices to communicate with one another without any interruptions [30]. The Internet of Things gives each device unique Internet Protocol (IP) addresses according to their specific requirements. These things are incorporated into more complicated systems, and sensors are used to collect data depending on certain conditions that are present in the surrounding environment. The information that has been gathered is subsequently sent, in accordance with the needs of the applications, now in use, to any nearby sensors. The Internet of Things makes it easier to aggregate and retrieve information that has been acquired by individual items or components of more complicated systems [31, 32].

Wireless Sensor Networks Wireless Sensor Networks, or WSNs for short, are an extra critical component of the Internet of Things. WSNs are most often referred to by their acronym. These networks are constructed up of interconnected sensors that extract information from the settings in which they are situated. The sensors are able to carry out wireless communication with one another, which makes it possible for data to be sent within the network. The information gathered from the sensors may be put to use in a variety of applications and services related to the Internet of Things.

Data Aggregation in IoT

Sensor nodes are carefully placed around the network in order to monitor and gather data on the surrounding environment. These nodes are responsible for storing the essential information and are the ones that directly encounter the environment. A communication strategy including many hops is used in order to send the data that has been captured further to the sink node. During this procedure, some nodes that are referred to as relay nodes are used in order to transfer the data that was sensed towards the node that is designated as the sink. In comparison to end devices, the processing capabilities of these relay nodes are much greater [33].

Applications of the Internet of Things that need frequent monitoring require the relay node to gather redundant data from child nodes. Because of this, only the data that are necessary are sent from the relay nodes to the sink node, rather than the superfluous values that would normally be transmitted in such scenarios. This optimization not only prevents the waste of energy but also guarantees the effective transfer of any necessary data [34].

The process of record aggregation is a technique that improves the effective utilization of available resources during the transmission of information. It may entail the consolidation of data or the grouping of data in order to reduce the total amount of information that must be communicated. By aggregating records, material that is redundant or otherwise similar may be integrated into a single set. This results in less bandwidth use and increased resource efficiency.

The models are shown in Fig. 4, wherein one image is with aggregation and different is without aggregation as inside the figure. The sensor nodes 1, 2, 3, 5, 6, and 7 are responsible for the collection of data from the environment in the models that have been shown here. These periodic sensor nodes collect data, which is subsequently passed on to nodes of a higher level, namely, nodes 4 and 8. Because they are responsible for the duty of aggregating the information packets that have been saved, nodes 4 and 8 are often referred to as relay or aggregator nodes. In the configuration that does not use data aggregation, the three information packets that were acquired by nodes 1, 2, and 3 are merged and sent on to the base station by node 4. In contrast, just one information packet is sent from the aggregator node 8 to the base station when the second version is used. This strategy aggregates the information packets before sending them on to the base station, which significantly reduces the amount of data that has to be sent.

This is the architecture of the data aggregation technique, which can be seen in Fig. 2. In this scenario, the sensor node transfers the observed data to the algorithm, which then aggregates the data using several aggregation protocols (such LEACH, LEACH, TAG, and many more). When the feature of in-network data aggregation is used, the data that has been aggregated from a variety of sensor nodes may be effectively transported to the base station through the way that is considered the most efficient. The base station is able to receive the aggregated data as a result of this, which is the data that has been gathered and merged from a number of different sources. Because of this, the data are successfully used and sent to the base station, which contributes to an improvement in the system's overall efficiency (Fig. 5).

The aggregation function may be broken down into many different pieces, which are described in more detail below:

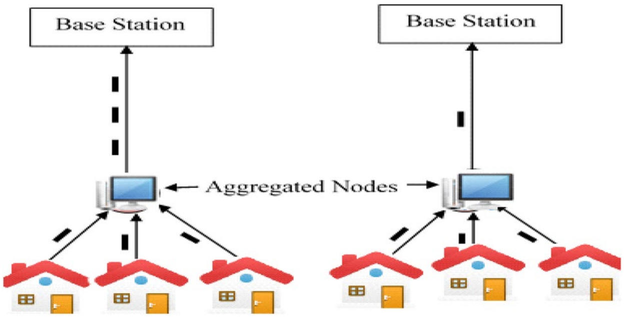


Fig. 4 Data models in the internet of things: those without and those with aggregation

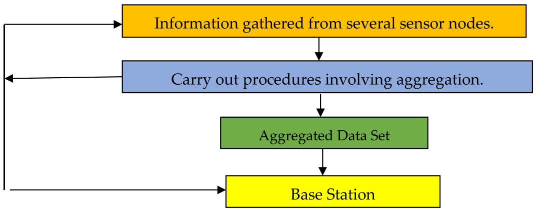

Information gathered from several sensor nodes.
Carry out procedures involving aggregation.
Aggregated Data Set
Base Station

Fig. 5 The basic components that make up the data aggregation algorithm

1. This sort of aggregation function is known as "duplicate insensitive" because it generates results that are unaffected by the presence of duplicate data. It zeroes into a single number to determine whether the minimum or maximum value (for example, min or Max) should be returned.
2. When the aggregated node receives numerous data packets that contain similar information as a result of correlation, the duplicate sensitive function kicks in and begins to operate. The ultimate outcomes of this function consider the counts of duplication, for example, when computing the average value (denoted by the symbol Avg).
3. In a process known as lossy aggregation, the original information cannot be reconstructed once it has been compressed. The compressed data does not keep the original information's precise details as they were.
4. Lossless: The goal of the lossless aggregation function is to maintain the integrity of the original data even after it has been compressed. It guarantees that any and all information may be correctly retrieved from the aggregated value in a way that is appropriate at the receiver side.

Organization of Papers

The study paper is broken up into five distinct sections, the first of which is an introduction that provides an all-encompassing overview of the subject matter of energy usage in IoT-based networks. Provides a literature review, which includes a summary of many different research publications that were carried out on the topic. Examines the work that was presented and lays out a flowchart and algorithm with the goal of reducing the amount of energy that was used. The offered material consists of a discussion of the results as well as a comparison of the suggested algorithms with those that already exist. The last section summarizes the findings of the article and discusses possible directions for further research.

Review of Literature

Author [34] presented the Energy-LEACH protocol, introducing the incorporation of a node's residual energy as the primary parameter for selecting cluster heads in subsequent rounds following the first. Their approach resulted in a notable reduction in the overall energy consumption across the network. Author [35] partitioned the monitored area into distinct cells, designating a single node as the Cell-Head for each. These Cell-Heads, forming clusters of seven cells each, transmitted their cell members' data to cluster heads. Through the integration of a node's residual energy into the cell-head and cluster-head selection process, they asserted the achievement of a more balanced energy distribution throughout the network.

An energy-saving method was developed by researcher [36] who modified the K-means algorithm. This modification led to an equally dispersed cluster layout and fair allocation of workloads across clusters in sensor networks. Within the framework of the EEE-LEACH protocol, Researcher [37] wanted to improve the effectiveness of the network by shortening the distances that separate individual nodes' communication channels. This was accomplished via the use of multi-level clustering. This protocol introduced the concept of Master Cluster Heads, in addition to regular cluster heads, effectively diminishing energy consumption in the transmission process. Author [38] proposed an optimized iteration of the LEACH-C protocol, enhancing network energy efficiency through the estimation of cluster head energy consumption using parameters such as the count of transmissions and acknowledgments.

In parallel with these endeavors, work [39] also strives to contribute to the realm of clustered wireless sensor networks. Our focus centers on achieving superior energy efficiency by leveraging innovative methodologies, aligning with the broader aim of optimizing the performance and sustainability of such networks.

Yogesh Seralathan et al. [40] emphasized the linked nature of Internet of Things (IoT) devices and the expanding usage of these devices in different applications, which leads to the gathering of large quantities of data daily. In addition, they highlighted the increasing use of these devices. However, since there are no security measures that have been applied, these devices are susceptible to assault. As a result, it is essential to make certain that adequate security measures are in place to safeguard the data from assault by malware.

Chalee Vorakulpipat et al. [41] brought attention to the considerable difficulty presented by devices as a result of their extensive usage, especially in commercial networks. As more people shift away from using desktop computers and towards using mobile devices, the stability of the network becomes a big problem. The authors discussed the problems and challenges associated with Internet of Things (IoT) security, taking into consideration the many IoT system resources that might change depending on the needs of a company.

In their research, Jesus Pacheco and colleagues [42] suggested an Internet of Things security architecture that was tailored to meet the unique requirements of the incorporation of a smart water system. The framework was composed of four levels, and it had a hazard model that could identify possible threats to each of those layers. The authors went on to explore other topics, including the security of the communications gateway, which is a vital part of the IoT system. Their strategy suggested using a profile to characterize the typical actions of the gateway, and they proved that it was useful in recognizing certain kinds of assaults with a low false positive rate and good recognition skills. Additionally, the proposed method resulted in a minor increase in overhead in terms of performance measures, which kept the gateway's regular operation intact.

Se-Ra Oh et al. [43] presented a collaborative Internet of things system that is both user-friendly and aware of its surrounding environment. The authors emphasized the significance of guaranteeing the safety of devices connected to the Internet of Things (IoT) and dealing with dangers that have a direct influence on the IoT system in light of the growing popularity of these devices. They spoke about a security design for one Machine-to-Machine (M2M) scenario, with the primary emphasis being on the provision of permission and authentication by means of a single Machine-to-Machine security component that was based on OAuth 2.0.

Mbanaso et al. [44] brought out the need of a flexible policy-based definition in order to address issues regarding privacy and the secrecy of trust in distributed settings. They emphasized how important it is to create trustworthy and secure smart organizations, and they provided a method for Internet of Things organizations to convey their needs and capabilities in a way that is coherent. In the context of the internet of things (IoT), this technique was successful in addressing problems like anonymity, security, and trust.

The problem of implementing cryptographic algorithms and protocols within the physical restrictions of IoT devices was brought to light in the 2018 study [45] written by Yiqun Zhang and colleagues. They paid attention to the challenges that are associated with putting software on IoT devices and stressed how essential it is to guarantee the safety of the Internet of Things (IoT). There are a number of problems that are linked with this circumstance; some of these problems include restrictions on bandwidth, a lack of flexibility in domain-specific accelerators, and resource overhead in reconfigurable cryptographic processors. The authors presented a customizable cryptographic processor that they termed "Recryptor." It maximizes the use of the available memory at a time and uses a 10-transistor bit cell for computations that occur in memory. Because of its close proximity to memory and modules such as shifter, rotator, and S-box, the Recryptor was able to exhibit high-throughput processing capabilities using a variety of bitwise operations that were up to 512 bits wide. Because it was programmable, the recryptor made it possible to enforce cryptographic primitives in an effective manner.

A complete stack of Internet of Things security items and techniques was described by Ibrahim R. Waz et al. [46]. The authors' goal was to create integrity across various IoT platforms and to assure continuity of security from one stage to the next. Their method of integration makes it possible to track data between users and Internet of Things devices in a smooth manner using middleware.

Israr Ahmed et al. [47] examined the tremendous influence that IoT has on our day-to-day lives and underlined the extensive use of this technology in both the virtual and physical domains.

Zhen Ling et al. [48] investigated the development of the Internet of things and its link to the internet. They focused on the rising network connectivity among a variety of different components. The number of individuals who use the internet has increased dramatically in recent years, reaching over 6 billion, and it is anticipated that this figure will eventually reach 20 billion devices.

In their study, Swapnil Naik and colleagues [49] brought attention to the fact that typical software security approaches for personal computers and mobile devices would not be enough for securing data in the Internet of Things. In the study, we explored real-world situations in which security cameras were hacked, which led to data breaches on platforms such as Twitter. This study aimed to find ways to reduce the risks associated with the Internet of Things (IoT), especially those associated with cloning devices and exposing sensitive data.

Aanchal Punia and colleagues [50] proposed a network of heterogeneous devices in the Internet of Things sector, with a primary emphasis on sensing, actuation, and wireless communication. Their goal was to ensure that all machinery and electronic equipment were permanently connected to one another. In the study, security and privacy concerns were analysed, current methodologies were examined, tests were carried out, and security difficulties were identified based on the results of the survey that was carried out.

Maryam Daud and colleagues [51] discussed the role that the Internet of Things (IoT) plays in automating equipment and its widespread use in day-to-day life, which is made possible by a variety of sensors. Interoperability can be improved by incorporating core Internet of Things technologies, but there is still a lot of opportunity for improvement in terms of data protection and security. The study paper examined the architecture of the Internet of Things (IoT) and discovered vulnerabilities and threats in its numerous levels, such as the application layer, the perception layer, the network layer, and the middleware layer. In order to maintain the data's secrecy, it was highlighted how important it is to maintain compliance with a set of predetermined security requirements. The article also provided ways to mitigate these dangers, offering appropriate security measures for IoT systems. These solutions were presented as part of the paper.

The difficulties that arise in the process of developing circuits for new memory devices, in particular nonvolatile memory (NVM) macros, were highlighted in Chunmeng Dou's and colleagues' [52] article. These memory devices have a wide range of applications in modern processors, and they also provide computing services and protection to devices that are connected to the Internet of things. The study analised of circuit designs for a variety of memory devices and included a review of silicon-verified samples. The primary emphasis of the analysis was on the difficulties that arose throughout the design process.

In order to protect the devices connected to the Internet of Things, Mohamed Tahar Hammi and his colleagues [53] developed a security protocol that is not only lightweight but also energy-efficient. The protocol offered integrity and secrecy for the data that was shared, as well as mutual authentication between the organizations who were talking with one another. To solve the problem of internal identity confusion, a personalized system was implemented. The suggested protocol created a secure channel in a short amount of time by making use of a symmetric encryption technique that was resilient, fast, and lightweight (AES GCM/CCM). It prevented cryptanalysis and replay attacks, allowing for communication that was both flexible and safe across various Cyber-Physical Area Networks (CPANs). The goal of the project was to create a communications system that was very safe for use by devices that were part of a CPAN-controlled network.

An exhaustive study of Internet of Things applications was carried out by Parul Datta and colleagues [54], who focused their attention on architecture, protocols, security, and smart cities. The fundamental aspects of Internet of Things architecture were first discussed in this study, with an emphasis placed on the application layer protocols that are used for communication. After that, it showed many application layer protocols and compared their capabilities and characteristics within the context of the Internet of Things (IoT). In addition, the authors highlighted a variety of Preventive safety measures and presented examples of applications based on smart city deployments.

Chinmaya Mahapatra and colleagues [55] presented a wireless system that they named the Internet of Things (IoT). This system makes use of a variety of protocols and devices in order to make it possible for machines and sensors to communicate with one another. The system is designed to accommodate real-time as well as virtual online sensors, and it offers capabilities for the collection of data, storage of data, connection with other systems, and processing of data inside IoT systems. In light of the increased interconnectedness and complexity of the Internet of Things (IoT), it is essential that client devices have effective energy consumption and reliable data transmission. In order to overcome these difficulties, the research article presented RFID tags that handle data based on Cluster Heads (CH) identification as well as energy harvesting approaches.

Mario Frustaci and colleagues [56] devised a solution to handle difficulties related to the transmission of data and energy efficiency in heterogeneous systems. Through the use of simulations, the suggested technique was able to show higher performance when compared to other methods already in use. In order to do this, the procedure requires the creation of energy consumption models for each cycle, considering the existence of several gateways. The suggested strategy is intended to increase the total network lifespan in heterogeneous systems by maximizing the efficiency of energy use.

In the realm of cybersecurity education, Kosuke Kaneko and colleagues [57] carried out a research in which they contrasted experience learning with non-experiential learning approaches in order to assess the efficiency of learning via the application of experimental data. The research was conducted using two distinct types of lectures, one of which included an experimental group to enhance research. Learners were presented with foundational information about cybersecurity by the presenter during the lecture formatted like a traditional classroom setting. After that, the students were broken up into groups and instructed to participate in a series of hands-on activities that included doing product trials and guarding against potential threats. The purpose of this study was to determine whether or not experiential learning is an effective method for improving cybersecurity education.

Chen Chen and colleagues [58] proposed in their study that implementing a power-saving scheduling scheme could significantly reduce the traffic meter's overhead scheduling in both the uplink and downlink on the Internet of Energy. Similarly, Mian Muhammad Ahmed and his colleagues [59] emphasized the remarkable progress of the Internet of Things (IoT) in the field of Information and Communication Technology (ICT), highlighting it as one of the fastest growing technologies. Because of the IoT's versatility, it is expected to include more than 50 billion devices in the coming years.

The authors Jyoti Deogirikar et al. [60] explored the Internet of Things (IoT) in their research work. This is a topic of technology that is well known and has a great deal of anticipation around it. Despite the fact that there have been considerable developments made in IoT and that it provides several advantages for a variety of applications, it does not come without risks. The authors address these weaknesses by investigating and categorising various assaults on the Internet of things (IoT), with the goal of discovering viable responses. They carried out a study of these assaults and assessed the efficacy of each one, which provided useful information for improving the security of IoT devices.

In a separate piece of research, Xiaosen Liu and colleagues [61] concentrate on energy harvesting as it relates to smart nodes in Internet of Things (IoT) networks. They recommend using a monolithic microwatt-level charge pump since it is the most effective way to give the necessary amount of energy. The authors optimize the charge pump architecture and circuit design by considering the different levels of voltage and power that are available. They use hybrid conversion ratios in a reconfigurable charge pump in order to cut down on charge redistribution loss as much as possible. The maximum power point tracking (MPPT) capability is enabled using frequency modulation, which also contributes to the establishment of a 2D MPPT system. The maximum power point tracking (MPPT) technique, when coupled with the constant-on-time (COT) scheme, is an approach to sensing that does away with the need for traditional means of delivering energy. The suggested technique displays, with the help of simulations, a straightforward and improved power conversion efficiency (PCE) for gathering energy from a wide variety of sources by making use of a significant number of intelligent nodes.

An elaborate network that enables the transfer of data through internet connections was developed by Mukrimah Nawir and colleagues (2016) [62]. This network is made up of intelligent gadgets that are incorporated inside the domain of the Internet of Things (IoT). A location-based solution that makes use of wireless systems was developed by Inzerilli et al. [63] as a way to handle smooth mobile-controlled vertical handovers. Yu et al. [64] proposed using the Recursive Principal Component Analysis (R-PCA) method inside a cluster-based data analysis framework. This will successfully mitigate the issues that were previously highlighted. In this approach, the data are combined using principle components (PCs) as they are being processed inside a cluster. The information is compiled by a member of the cluster while being supervised by the head of the cluster. After the principal components had been extracted, a score known as the Anomalous Squared Prediction Error (SPE) was used in order to find probable data outliers. This score is also known as the square of the residual value. The Internet of Things (IoT) has been given the ability to improve the parameters of the PCA model in the network as a result of the incorporation of R-PCA.

Lu et al. (2017) [65] proposed in this paper, there are many techniques that implemented in the network for the characterization of the proposed method. So, by the help of this method easily false data can be found. For the evaluation of the proposed method, experiments were done that shows the effectiveness of the method which is lightweight in fog computing-enhanced IoT.

An Improved Network Aggregation and Distribution of Conditional IoT Subscription Solution (INADS) was presented by Dong et al. [66] to be utilised for Information-Centric Networking (ICN). Therefore, in contrast to the other ways, this approach is the most suitable for future implementations. The number of non-certifications will be reduced in both single- and multiple-producer situations if this strategy is used. The advantage of this method leads to the minimization of power consumption S. Bhandari et al. [67]. Thus, it is required to decrease the bandwidth consumption and a reduction in the notification messages for transmitting subscription messages.

In this study, U. S. Thakare and colleagues (2017) [68] offered an Internet of Things-based network solution to handle a variety of difficulties. They used a hash-based addressing technique to simplify data aggregation in IoT devices, which ultimately resulted in a reduction in the amount of power that was used. They created an authentication system based on Kerberos in order to guarantee the control of the electricity. They placed an emphasis on monitoring and safety by using an ecosystem based on the Internet of Things. In addition to this, they designed a reconfigurable smart sensor interface by making use of a Complex Programmable Logic Device (CPLD) as the primary controller. The use of this interface made it possible to get data in real time from a variety of sensors deployed across the surroundings. Both the IEEE 1451.2 standard for intelligent sensor interface requirements and solutions for generic sensor data collection were provided by the authors. Their strategy included combining the industry standard IEEE 1451.2 with cutting-edge programmable CPLD technology.

Proposed Framework

In the context of Wireless Sensor Networks (WSNs), achieving a balanced distribution of energy consumption among nodes is of paramount importance due to its direct impact on network performance. The equitable allocation of power usage across nodes stands as a critical challenge within such networks. The energy dissipation of a node is influenced by several variables, including its proximity to the Base Station (BS) or Sink, the volume of data transmitted by the node (whether it's transmitting solely its own data or acting as a data collector and forwarder for other nodes), and the duration of each transmission undertaken by the node. These varying parameters lead to an uneven energy consumption pattern among nodes, necessitating techniques to adjust and optimize them to extend the network's lifespan. However, this task is far from straightforward due to the decentralized nature of WSNs and the constraints posed by limited and non-replaceable batteries. The intricate interplay of these factors renders the energy optimization challenge exceedingly complex and demanding. To address this, clustering schemes emerge as a promising avenue for enhancing energy efficiency within the network. These schemes capitalize on the resource constraints of sensor nodes, necessitating simplicity, scalability, and robustness in their algorithms. An effective clustering scheme should be capable of mitigating both inter-cluster and intra-cluster interference, while minimizing the overall communication overhead. Central to this research landscape is the quest to devise an energy-efficient and load-balanced clustering scheme tailored for WSNs. The objective is twofold: to conserve energy and promote a uniform distribution of energy utilization across network nodes. Achieving this balance holds the potential to significantly prolong the network's operational lifespan, making it a pivotal research frontier. In addressing this issue, researchers delve into the intricacies of WSNs, striving to formulate clustering techniques that effectively optimize energy consumption. The challenge lies in navigating the delicate equilibrium between energy-efficient operation and maintaining an equitable load distribution. This endeavor demands innovative strategies that harness the unique characteristics of WSNs while circumventing their inherent limitations. As the WSN landscape continues to evolve, the quest for a robust and efficient clustering scheme gains even more significance. Researchers strive to strike the ideal balance between energy conservation, load distribution, and network performance. The outcome of these efforts could potentially reshape the trajectory of WSNs, enabling sustainable and optimized operation in resource-constrained environments.

Limitations within LEACH

The deficiencies present in the LEACH protocol stem from various technical aspects:

1. **Random Cluster Head Selection**: The practice of randomly selecting cluster heads in each round gives rise to a substantial imbalance in energy consumption across different nodes within the network. This randomness can lead to situations where certain nodes are frequently chosen as cluster heads, causing them to deplete their energy rapidly and rendering them inactive for subsequent rounds.
2. **Neglect of Distance from Base Station:** LEACH's cluster head selection process doesn't account for a node's distance from the base station (BS). Consequently, nodes situated far from the BS, which are required to undertake long-range transmissions, experience accelerated energy consumption. This inefficiency undermines the network's overall energy utilization.
3. **Lack of Energy-Aware Cluster Head Formation:** The distributed process of selecting cluster heads doesn't consider the residual energy of a node. As a result, nodes with limited energy might be designated as cluster heads, potentially leading to a scenario where these nodes lack the energy capacity to transmit aggregated data to the BS effectively.
4. **Cluster Size Variability:** LEACH's usage of varying cluster sizes directly influences the energy consumption profiles of the respective cluster heads. This discrepancy in energy usage among cluster heads can result in uneven depletion rates, exacerbating network instability.
5. **Unpredictable Cluster Head Count:** LEACH employs a probability-based selection method to choose cluster heads, leading to an indeterminate number of cluster heads in each round. This unpredictability contributes to an unstable network structure, making resource allocation and management more intricate.

These technical shortcomings collectively impact the energy efficiency, stability, and longevity of the network. Addressing these inadequacies becomes crucial in the pursuit of developing an enhanced and optimized routing protocol for Wireless Sensor Networks.

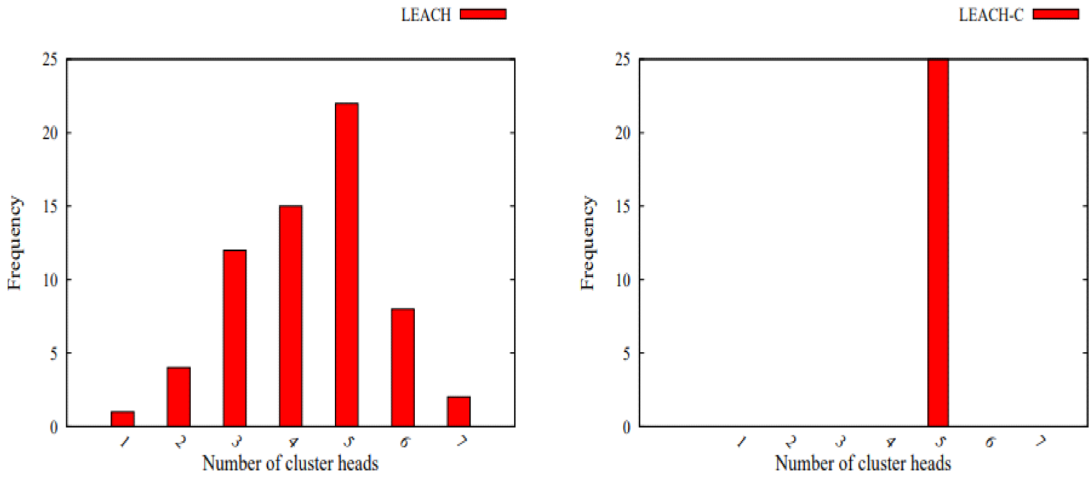
LEACH-C

In the paper LEACH-C [40], the authors provide a strategy that may be used to overcome this obstacle. In this particular protocol, the base station is responsible for designating a certain number of nodes as the cluster leaders for each round. However, the precise number of nodes that are connected to separate cluster heads might change from round to round (this is referred to as the cluster size). Within the LEACH-C architecture, the frequency of nodes playing the part of cluster heads stays the same throughout all of the rounds, as seen in Fig. 6.

Both the steady-state phase of the LEACH reaction and the steady-state phase of the LEACH-C reaction are quite comparable to one another. At some point in the process of establishing the network, each of the nodes will communicate with the base station (BS) in order to relay information on their current amounts of energy and locations. The BS receives an all-encompassing knowledge of the present status of the network as a result of this. Through this data, the average energy of the network ($\boldsymbol{E_{Avg}}$) is computed by the BS. Nodes possessing energy levels surpassing ($\boldsymbol{E_{Avg}}$) are qualified to undertake the role of a cluster head (CH) for the ongoing round. Subsequently, the simulated annealing technique [62] is employed to orchestrate the formation of clusters. The cluster formation details are then disseminated to sensor nodes, which utilize the broadcasted information to make individual decisions, designating themselves either as a CH or a cluster member (CM) within their assigned cluster. To establish synchronization, all CHs formulate a Time Division Multiple Access (TDMA) schedule for their respective CMs. Upon receipt of this schedule, the CMs initiate data transmission during their allocated time slots to their respective CHs. While LEACH-C effectively addresses the issue of fluctuating cluster head counts over multiple rounds, the inherent randomness in the cluster head selection process continues to introduce an uneven distribution of energy consumption among nodes. Given that a cluster head expends its energy at an accelerated rate, repeated selection of the same node as a CH for multiple rounds could lead to its premature depletion and eventual inactivity. To mitigate these concerns, this chapter introduces a refined solution aimed at achieving a more equitable distribution of energy consumption across the network compared to LEACH-C. By leveraging this enhanced approach, the aim is to minimize the adverse effects of uneven energy dissipation and foster a more robust and balanced network operation.

Proposed Energy Efficient Clustering Scheme

The strategy that has been suggested is an enlargement of the LEACH-C framework, and its primary objective is to improve energy efficiency. This technique, which is analogous to LEACH and LEACH-C, is built on the foundation of two essential phases: the initialization phase and the steady-state phase. Through the use of the following tactics, we want to accomplish our major objective, which is to achieve energy efficiency while simultaneously increasing the lifetime of the network:



(a) Cluster Head frequency in LEACH

(b) Cluster Head frequency in LEACH-C

Fig. 6 Analysis of LEACH and LEACH-C protocol with head frequency

1. Our strategy tries to minimize the amount of energy that is used during the transmission of data packets from cluster members (CM) to the cluster heads (CH) of their respective clusters. The distance between the transmitting node (CH) and the receiving node (CM) is directly proportional to the amount of energy needed for the transmission. The entire energy usage may be brought down to a more manageable level by reducing the distance between these two points.
2. Choosing a Cluster Head Is Done According to Its Level of Remaining Energy The nodes in a cluster that have the greatest level of remaining energy are the ones that are chosen to be the cluster heads. This selection criterion guarantees that cluster chiefs are able to successfully handle their tasks without experiencing an early drain on their energy levels.
3. The protocol identifies nodes as cluster heads if they match two specified criteria: having both more residual energy and a shorter distance from the Base Station (BS). This allows for optimized cluster head selection. This dual strategy tries to capitalize on the benefits of closeness to the BS while also ensuring considerable volumes of energy are maintained.
4. Our innovative approach to clustering, which was conceived with the aforementioned ideas in mind, is geared towards accomplishing the goals that were presented earlier. Our strategy provides a more streamlined method for clustering nodes within the network by giving priority to the transmission of data in an energy-efficient manner, optimizing the selection of cluster heads via the evaluation of residual energy, and incorporating proximity to the BS as a consideration in decision-making. This comprehensive method has the purpose of extending the lifetime of the network, reducing the amount of energy that is wasted, and improving the overall performance of the LEACH-C protocol.

Energy Consumption Calculation

The accurate modelling of energy consumption is of the utmost relevance in the field of energy-efficient routing, as it allows knowledgeable routing choices with a strong energy-conscious emphasis and is thus of the utmost value.

Using Eqs. (2), (3), (4) and (5), the total amount of energy that is used by a cluster head for the whole of the data collecting, aggregation, and transmission operations can be stated as follows:

$$E_{CH} = \ell \cdot E_{\text{clec}} \cdot \left(\frac{n}{k} - 1\right) + \frac{n}{k} \cdot \ell \cdot E_{da} + l \cdot \varepsilon_{fs} \cdot d_{BS}^2 \tag{2}$$

When the results of Eqs. (1.7) and (3.1) are plugged into Eq. (1.8), we can determine the total amount of energy that is used by a cluster, which can be written as:

$$E_{Cluster} = \ell \cdot \left(2 \cdot E_{\text{elec}} \cdot \left(\frac{n}{k} - 1\right) + \frac{n}{k} \cdot E_{da} + \varepsilon_{fs} \cdot \left(d_{CH}^2 + d_{BS}^2\right)\right) \tag{3}$$

The whole network's cumulative energy consumption over the duration of a single round may be broken down into the following categories, provided that our assumptions about the number of clusters that exist inside a single round hold true:

$$E_{\text{Round}} = \sum_{i=1}^{k} E_{\text{Cluster}}(i) \tag{4}$$

After plugging in the result that was obtained from Eq. (3.2), we get the following:

$$E_{\text{Round}} = \ell \cdot \left(2 \cdot E_{\text{clec.}}\,(n-k) + n \cdot E_{da} + \sum_{i=1}^{k} \varepsilon_{fs} \cdot \left(d_{CH}^2 + d_{BS}^2 \right) \right) \tag{5}$$

The progression of clusters correlates to various modifications in rounds within the equation that has been provided. Despite these changes, several elements continue to be the same, with the exception of 'd_{BS}' and 'd_{CH}'. Throughout the different rounds, it becomes clear that the function of the cluster head (CH) is a very important one, particularly with respect to the data transfer for the other nodes. The following three conditions must be met in order to ensure that the transmission process uses the least amount of energy possible: Reduced the amount of distance between CH and BS. The distances between each member of the cluster and the head of the cluster have been cut down as much as possible.

A sufficient amount of unused energy must be present in the CH in order for the data transfer to the BS to be successful.

In order to overcome these concerns, we propose a unique method for selecting cluster heads that takes into account the following three important parameters:

- The remaining energy of a single node, abbreviated as "E_{res}."
- The distance between the Base Station and the CH is denoted by d_{BS}.
- The distance from node 'i' to the CH is denoted by the variable $d_{i(CH)}$.

Our discussion will focus on two separate plans, each of which is described in more depth in the following subsections:

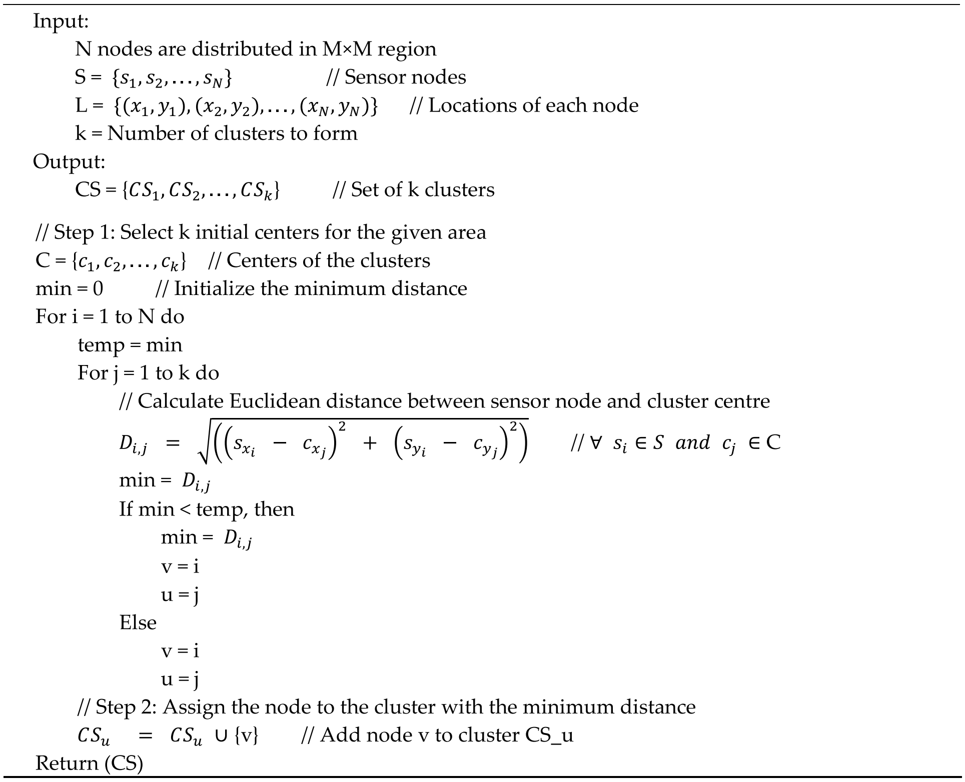
1. The node with the greatest residual energy (referred to as LEACH-CE) will be chosen.
2. The node with the highest residual energy and the shortest distance to the BS will be chosen for the BSLEACH-CE step.

These schemes need the beginning of the cluster formation process, which is an essential component of the protocol that we have presented. The procedure is comprised of two basic components: the construction of clusters and the selection of cluster heads. In the first part of the process, the base station will gather data on the level of energy and position from all of the sensor nodes. After then, the base station is responsible for two primary responsibilities, which are as follows:

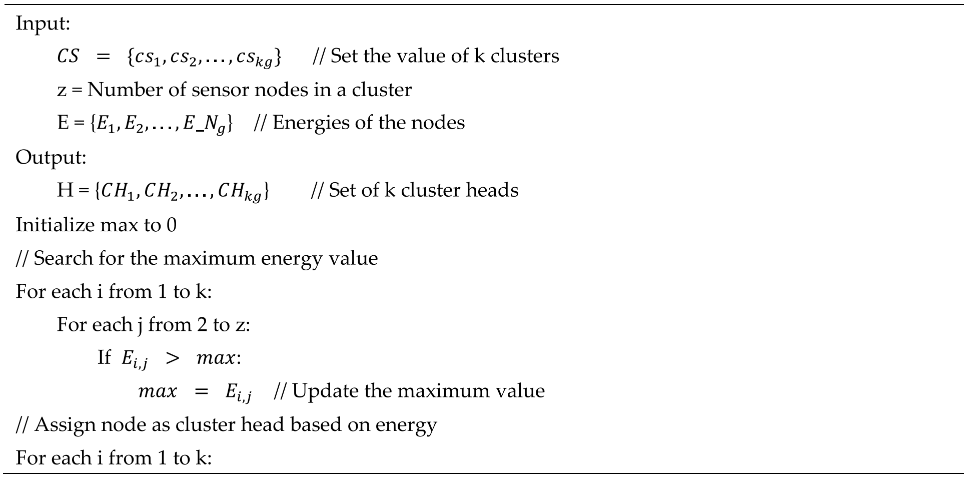
1. By forming clusters out of nodes that are physically close to one another, one may reduce the amount of energy required for data transit while also saving money.
2. Locating the node that serves as the cluster head for each cluster.

In order to begin the process of forming clusters, the base station will first choose 'k' cluster centres. These centres are meant to represent geographic places that are crucial to the network but do not necessarily need to correlate to the positions of any sensor nodes. The next thing that has to be done is to figure out the distance that separates each sensor node and each cluster centre. The node is placed in the centre of the cluster that is the furthest away from it, and thus helps to reduce the value of the metric known as '$d_i(CH)$' by clustering nodes that are physically close together. This process is carried out for each node by the base station, which eventually results in the formation of clusters. The full method for this procedure may be found in method of algorithm 1.

The process of selecting a cluster head begins after the clusters have been created and are functional. The function of cluster head for a round is given to the node that has the largest total amount of remaining energy. This process is carried out again at the beginning of each cycle in order to identify the next cluster head. In order to make this process easier, the base station is the one who collects the values of the nodes' remaining energy at the beginning of each loop.



```
Input:
    N nodes are distributed in M×M region
    S = {$s_1, s_2, \ldots, s_N$}            // Sensor nodes
    L = {$(x_1, y_1), (x_2, y_2), \ldots, (x_N, y_N)$}    // Locations of each node
    k = Number of clusters to form
Output:
    CS = {$CS_1, CS_2, \ldots, CS_k$}      // Set of k clusters
// Step 1: Select k initial centers for the given area
C = {$c_1, c_2, \ldots, c_k$}    // Centers of the clusters
min = 0        // Initialize the minimum distance
For i = 1 to N do
    temp = min
    For j = 1 to k do
        // Calculate Euclidean distance between sensor node and cluster centre
        $D_{i,j} = \sqrt{\left(\left(s_{x_i} - c_{x_j}\right)^2 + \left(s_{y_i} - c_{y_j}\right)^2\right)}$     // ∀ $s_i \in S$ and $c_j \in$ C
        min = $D_{i,j}$
        If min < temp, then
            min = $D_{i,j}$
            v = i
            u = j
        Else
            v = i
            u = j
    // Step 2: Assign the node to the cluster with the minimum distance
    $CS_u = CS_u \cup$ {v}     // Add node v to cluster CS_u
Return (CS)
```



```
Input:
    $CS = \{cs_1, cs_2, \ldots, cs_{kg}\}$     // Set the value of k clusters
    z = Number of sensor nodes in a cluster
    E = {$E_1, E_2, \ldots, E\_N_g$}   // Energies of the nodes
Output:
    H = {$CH_1, CH_2, \ldots, CH_{kg}$}      // Set of k cluster heads
Initialize max to 0
// Search for the maximum energy value
For each i from 1 to k:
    For each j from 2 to z:
        If $E_{i,j} > max$:
            $max = E_{i,j}$   // Update the maximum value
// Assign node as cluster head based on energy
For each i from 1 to k:
```

LEACH-CE technique, which is being presented as a new method in this context, is outlined in Algorithm 2, which can be found here. This LEACH-CE approach is shown in great detail in Algorithm 2, which can be found here. The mismatch in distances that exist between the sensor nodes and the base station causes a considerable difference in the amounts of energy that are used by each of the sensor nodes [107]. This is especially true for the cluster heads. Because of the disparity in distances between the sensor nodes and the base station, the sensor nodes have an uneven distribution of energy consumption, which has a particularly negative effect on the cluster heads. In addition, the distance that a cluster head is from the base station has a substantial impact on the amount of energy that it has left. The BSLEACH-CE technique uses a strategy that entails picking cluster heads based on their high residual energy as well as their closer proximity to the base station. This is done in order to remedy the problem that has been identified. Algorithm 3 provides a comprehensive breakdown of the BSLEACH-CE framework's method for selecting cluster leaders to serve as cluster heads. This strategy intends to improve the sensor network's performance in terms of both the utilization of energy and the efficiency of communication.

```
Input:
    α and β are constant weights
    CS = $\{c_{s1}, c_{s2}, \ldots, c_{skg}\}$    // set of k clusters
    z = sensor nodes in a cluster
Output:
H = $\{CH_1, CH_2, \ldots, CH_{kg}\}$
For each i from 1 to k:
    For each j from 2 to z:
        // Calculate Euclidean distance to base station
        $dBS(i,j) = sqrt((x_{i,j} - x_{BS})^2 + (y_{i,j} - y_{BS})^2)$

        // Assign default weights to α and β
        α = s
        β = s // Where 0 < s < 1 and α + β = 1
        // Calculate combined score using weights α and β
        $b(i,j) = \alpha * E_{i,j} + \beta * dBS_{i,j}$
Initialize max to 0
```

Performance Evaluation

Expanding the features of the NS-2 Network Simulator allowed us to evaluate how well the suggested techniques would function [8]. As part of this extension, the MIT unAMPS project [7] was integrated into the NS-2 platform. This gave us the opportunity to make changes to the already established LEACH implementation. Following that, we carried out simulations using LEACH, LEACH-C, LEACH-CE, and BSLEACH-CE, with all of the simulation settings being the same. We used a standardized set of circumstances for the assessment procedure and carried out a complete comparison of the results of simulations across all of these protocols. With this strategy, we were able to conduct a comprehensive investigation of the performance of the different procedures in a regulated setting and compare their results.

Experimental Set-Up

The experimental setup includes a network that is made up of one hundred stationary nodes, all of which are spread out over a square area that is one hundred square meters on each side. The Base Station (BS) is located outside the scope of this particular region. It is anticipated that none of the nodes will move. Our simulations take into account a wide

Table 1 Simulation parameters

Parameter name	Value
Number of nodes	100
Number of cluster heads	5% of total nodes
Round time	20 Sec
Simulation time	3600 Sec
Network area	100 × 100
Initial energy of nodes	2 Joule
Location of BS	(50, 175)

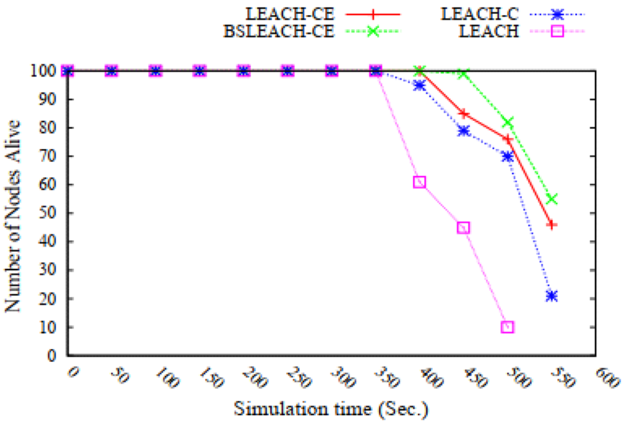


Fig. 7 Comparison of the total number of active nodes in LEACH, LEACH-C, BSLEACH-CE and LEACH-CE

variety of factors, which are detailed in Table 3.1. In order to verify that our system is resilient, we run simulations using 25 different possible random topology configurations. After then, the data that was generated are averaged so that there is a solid basis for further study. LEACH protocol can optimize its performance and energy efficiency by carefully considering topology considerations, including clustering, path selection, load balancing, adaptive routing, network partitioning, topology awareness, node mobility, security considerations. Table 1 provides an in-depth analysis of the simulation settings that were used throughout the course of our research. Because the averaged results provide a typical view of system performance, our analytical inquiry is based on the data that was acquired from these 25 different simulation instances. This data provides the foundation for our research.

Metrics Regarding Performance

The following types of performance measurements will be used in the course of evaluating the technique that has been suggested:

1. This real-time measure gives insight into the count of nodes that do not yet had their energy resources exhausted, and it is referred to as the "number of alive nodes." It gives an immediate measurement of the vitality of the network.
2. FND (First Node Death), HND (Half Node Death), and LND (Last Node Death): These metrics assess the timing disparity between the initiation of network operation and significant node events, such as the death of the first node, when 50% of nodes have depleted their energy (half node death), or the demise of the last node in the network. Other significant node events include: the death of the last node in the network.
3. This statistic calculates the mean amount of energy reserves that are kept by all nodes inside the network at a certain moment in time. It is referred to as the average network residual energy. It provides a holistic perspective on the manner in which the network distributes energy.
4. Deviation in Residual Energy The standard deviation of residual energy across 'n' nodes within the network is a measure of energy heterogeneity. Residual energy is the energy that is left over after work has been done. This deviation evaluation assists in determining the level of energy discrepancy that exists between the various nodes of the network [79].
5. We get a thorough comprehension of the performance of the suggested method by making use of a wide variety of performance indicators, taking into account aspects such as the lifetime of the network, the distribution of energy, and the general stability of the system.

$$\phi = \frac{\sqrt{\sum_{i=1}^{n}\left(E_i - \mathrm{E}\right)^2}}{(n-1)}$$

where E_i is residual energy of a node while $\overline{E}$ is the average energy of the network at a point of time.

Analysis of Results

Figure 7 shows a graphical representation of how the fraction of active sensor nodes in the network has increased over time. This figure demonstrates that at the beginning phases of the process, the performance of all of the different plans is similar. Nevertheless, as more time passes, LEACH-CE and Base Station (BS) LEACH- CE (BSLEACH-CE) perform better than the other available options. Within LEACH-C, the cluster heads are selected using a random selection process from the pool of possible candidates. Therefore, if the same node is frequently identified as a cluster head, the

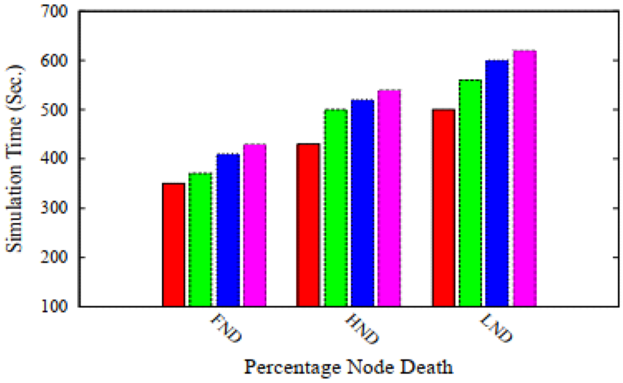


Fig. 8 Comparative Analysis of First Node Death (FND), Highest Node Death (HND), and Lowest Node Death (LND) across Various Protocols

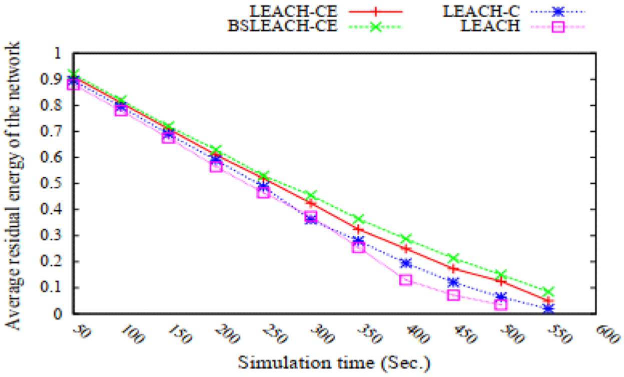


Fig. 9 The Change in the Typical Amount of Residual Energy Seen Across Protocols Over Time

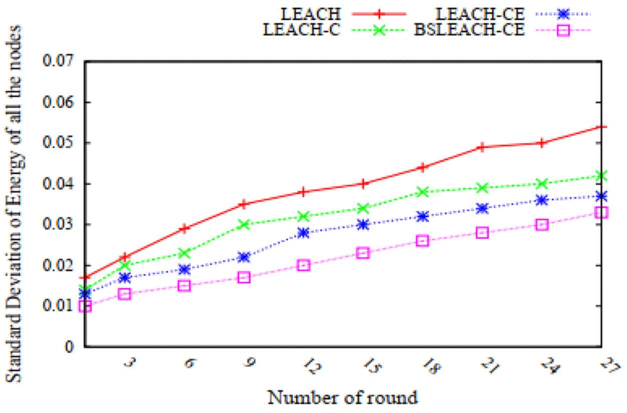


Fig. 10 Variation in Average Residual Energy Across All Nodes for Each Round According to the Standard Deviation

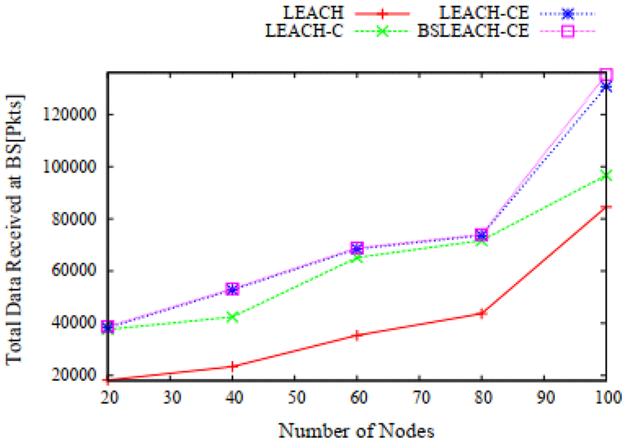


Fig. 11 Shows a Comparative Analysis of Different Proposed Schemes Using LEACH for Different Numbers of Nodes in the Network

energy of that node will decrease very quickly. On the other hand, one may achieve significant energy saving by carefully selecting the cluster heads to be used, in particular during the data transfer to the BS. This method is shown in the higher performance of both LEACH-CE and BSLEACH-CE, with their curves continually positioned above those of LEACH and LEACH-C. This energy-efficient strategy was used by both companies. Surprisingly, BSLEACH-CE obtains performance that is even superior than that of LEACH-CE. This improvement may be linked to the use of energy resources in a manner that is more equal. As a direct result of this, BSLEACH-CE maintains a lower rate of node depletion, which is shown by the fact that its curve is more above that of LEACH-CE.

It is essential to keep in mind that the functionality of the network is terminated whenever the number of dead nodes reaches a threshold that has been defined, such as the threshold of 96 nodes that was created in our example. This important insight brings to light the decisive role that energy management methods play in determining the lifetime of a network and its operational stability.

Figure 7 presents a chart that shows a comparison of the total number of active nodes throughout the course of time. This graphic demonstrates how resilient the network is when subjected to a variety of protocols. In Fig. 8. These insights were gathered from 25 unique random topology scenarios and evaluated under all protocols. After doing more research, it was found that the FND time in LEACH-CE and BSLEACH-CE was much longer than that of LEACH, by 14.6% and 16%, respectively. When compared to LEACH-C, this increase is shown to extend further, with LEACH-CE and BSLEACH-CE having FND times that are 9.7% and 11.9% larger than LEACH-C, respectively. The BSLEACH-CE displays a tremendous improvement when the lifespan of the network is taken into consideration. BSLEACH-CE has a lifespan that is 6% longer than that of LEACH-C, and its longevity is greater than LEACH's by more than 19% when it comes to the scenario of Half Node Death (HND). Figure 3.3 provides a clear illustration of the significant disparity in network longevity described above. The inferences that can be derived from these numbers illustrate the concrete benefits afforded by LEACH-CE and BSLEACH-CE in terms of network endurance, highlighting their ability to greatly prolong network operation before coming into contact with critical node depletion thresholds. These advantages can be seen in the figures.

After each cycle, the energy consumption of all of the nodes in the network, in addition to the average energy consumption throughout the network, is meticulously calculated. Given that cluster heads need a bigger energy allocation for packet transmission than ordinary sensor nodes, adopting a strategy that picks nodes with closer proximity to the Base Station (BS) and higher remaining energy as cluster heads may result in significant energy savings. This is because cluster heads are required to allocate more energy than regular sensor nodes. As can be seen in Fig. 9, it is clear that regardless of how long the simulation is run for, BSLEACH-CE always manages to keep the residual energy levels at their greatest possible levels. In addition, when compared to LEACH and LEACH-C, LEACH-CE demonstrates performance that is much superior. In order to conduct a more in-depth analysis of the energy distribution, the Eq. 3.5 is used to determine the standard deviation of the residual energy. Figure 10 demonstrates that the standard deviation of the residual energy stays consistently low for both suggested approaches throughout each and every cycle. This is an important finding. When compared to LEACH and LEACH-C, where larger standard deviations suggest a bigger energy imbalance across nodes, this finding stands in stark contrast. These results highlight the energy-efficient characteristics of both BSLEACH-CE and LEACH-CE, highlighting their potential to improve overall network performance, encourage more equitable energy utilization, and ultimately increase the network's overall sustainability.

In Fig. 11, we compare the two suggested techniques with the LEACH protocol that is currently in use over a range of different node counts. Notably, the efficiency with which data is sent to the Base Station (BS) shows a discernible rise, not only in BSLEACH-CE but also in LEACH-CE.

Discussion

This work has proved to be a significant useful in providing more balanced energy consumption patterns accepted by the proposed novel systems. The advantages of these techniques become even more obvious when the number of nodes in the network rises, which ultimately results in improved data transfer performance in comparison to the performance of standard protocols. Two alternative strategies have been developed to increase the energy efficiency of wireless sensor networks while preserving the fixed power constraints of sensor nodes. The first method, LEACH-CE, adopts the method of estimating the distance between sensor nodes and calculates the remaining energy levels to select cluster heads. This method effectively extends the life of the connection. Our simulation studies on a variety of random topologies demonstrate the flexibility of our method to different network configurations. The second method, BSLEACH-CE, further considers the geographical locations of nodes when selecting cluster heads. This selection process complements the LEACH-CE principles. Our proposed work also shows handling network Dynamics as the clustering structure is dynamically adjusted by using optimization algorithms, data routing and energy management.

The protocol also considers residual energy of nodes when selecting cluster heads by equally distributing the workload among nodes and also work on reducing distance traveled by data packets, minimizing energy consumption. The protocol employs data aggregation at cluster heads, reducing the amount of data transmitted to the base station. These further conserves energy by minimizing the number of transmissions.

Conclusion

We have discussed two novel strategies that have been designed to improve the energy efficiency of wireless sensor networks while still adhering to the strict resource limits of sensor nodes. The use of renewable forms of energy is a primary focus of these programmers, which result in significant advantages. LEACH's ability to adapt to changing network conditions is critical to its reliability and stability. With its dynamic flexibility and its clustering structure, load balancing, and routing protocols, LEACH can maintain data transmission and energy efficiency even as the network topology or node distribution evolves. In the first method, known as LEACH-CE, cluster heads are designated in a strategic manner by calculating the distance between sensor nodes and evaluating the amount of energy that has been left over. The lifetime of the network may be successfully extended using this strategy. Our simulation studies, which were carried out over a wide variety of random topologies, highlight the adaptability of our approach to a wide variety of different network configurations. When picking cluster heads using the second method, known as BSLEACH-CE, the geographical positions of the nodes are further taken into consideration. This selection procedure is complementary to the LEACH-CE principles that are put into use. Nodes that are physically farther away from the base station have to waste more energy overall in order to complete the transmission process than nodes that are physically closer. We are able to optimize cluster head placements and reduce overall network energy usage by including this geographical feature into the optimization process. The results of the simulations unequivocally show that our suggested algorithms provide significant gains in network longevity, improvements that are superior to those produced by current protocols by up to 10%. The findings provide further evidence that our proposed methods are effective and demonstrate their potential to considerably improve network lifetime and energy efficiency while simultaneously avoiding the imposition of unnecessary loads on the limited resources present in sensor nodes.

Acknowledgements NA.

Data availability The data supporting this study's findings are available from the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors declare no competing interests.

Consent to participate The authors declare their consent to participate in this article.

Consent for publication The authors declare their consent to publish this article.

Ethics approval Not applicable.

References

1. O. Vermesan SINTEF, Norway, Dr. Peter Friess EU, Belgium, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", *river publishers' series in communications, vol. 9*, issue 4, pp. 25–30, 2013.
2. O. Vermesan SINTEF, Norway, Dr. Peter Friess EU, Belgium, "Internet of Things–From Research and Innovation to Market Deployment", *river publishers' series in communications, vol. 15*, issue 8, pp. 125–130, 2014.
3. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, "Internet of Things Strategic Research Agenda", *Chapter 2 in Internet of Things -Global Technological and Societal Trends, River Publishers, vol. 4*, issue 1, pp. 54–66, 2011.
4. M. Serrano, Insight Centre for Data Analytics, Ireland, Omar Elloumi, Alcatel Lucent, France, Paul Murdock, Landis+Gyr, Switzerland, "Alliance for Internet of Things Innovation, Semantic Interoperability", *Release 2.0, AIOTI WG03 – IoT Standardisation, vol. 5*, issue 5, pp. 15–30, 2015.
5. Serrano M, Barnaghi P, Cousin FCP. OvidiuVermesan, Peter Friess, "Internet of Things Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps." European research cluster on the internet of things, IERC. 2015;9(2):18–35.
6. Rose K, Eldridge S, Chapin L. The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World. The Internet Society (ISOC). 2015;11(6):16–30.
7. B. Shanmuga Sundaram, "A quantitative analysis of 802.11ah wireless standard," *International Journal of Latest Research in Engineering and Technology, vol. 2*, issue 7, pp. 25–30, 2016.
8. Sun W, Choi M, Choi S. Ieee 802.11 ah: a long range 802.11 wlan at sub 1 ghz. J ICT Standard. 2013;1(1):83–108.
9. Baronti P, Pillai P, Chook VWC, Chessa S, Gotta A, Hu YF. Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards. Comput Commun. 2007;30(7):1655–95.
10. H. Liu, M. Bolic, A. Nayak, and I. Stojmenovi´c, "Taxonomy and challenges of the integration of RFID and wireless sensor networks," *IEEE Network, vol. 22*, no. 6, pp. 26–32, 2008.
11. A. Mitrokotsa and C. Douligeris, "Integrated RFID and sensor networks: architectures and applications," in RFID and Sensor Networks: Architectures, Protocols, Security and Integrations, pp. 511–535, *Auerbach Publications, vol. 19*, issue 4, pp. 18–56, 2009.
12. M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the internet of things", in *Proceedings of the 13th International Conference on Collaboration Technologies and Systems (CTS '12)*, pp. 21–26, Denver, Colo, USA, May 2012.
13. Krishna K, Ayan B, Mukherjee T, Gupta S. Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. Proc IEEE. 2012;9(4):25–34.
14. Kushner D. The Real Story of Stuxnet, How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. IEEE Spectr. 2013;6(4):17–30.
15. Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T. Comprehensive experimental analyses of automotive attack surfaces. USENIX Conference on Security. 2011;11(4):17–30.
16. Annaswamy M, Malekpour R, Baros S. Emerging research topics in control for smart infrastructures. Annu Rev Control. 2016;9(4):23–30.
17. Buckman A, Myfield S, Beck M. What is a Smart Building? Smart and Sustainable Built Environment. 2014;3(2):92–109.
18. Wang Z, Wang L, Dounis A, Yang R. Multi-agent control system with information fusion-based comfort model for smart buildings. Appl Energy. 2012;99:247–54.
19. M. Sadiku, S. Musa, O. Momoh, "Cloud Computing: Opportunities and Challenges", Potentials, *IEEE, Volume: 33*, Issue: 1, 2014.
20. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of Things: Vision, applications and research challenges. Ad Hoc Netw. 2012;10(7):1497–516.
21. Keyur K Patel, Sunil M Patel2, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", *IJESC, vol. 6*, issue 4, pp. 25–55, 2016.
22. Ruggier M. Homayounnikookar, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems." IEEE. 2013;5(2):14–30.
23. Mohammeda ZKA, Ahmed ESA. Internet of Things Applications, Challenges and Related Future Technologies. World Scientific News. 2017;7(4):18–44.
24. Daiwat A. Vyas, Dvijesh Bhatt2, DhavalJha, "IoT: Trends, Challenges and Future Scope." IJCSC. 2015;9(5):23–30.
25. Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim, Abaker Targio Hashem, FaizAlotaibi, "Internet of things Security: A Survey", *vol. 35*, pp. 25–30, 2017.
26. Ahamed J, Rajan AV. Internet of Things (IoT): Application Systems and Security Vulnerabilities. Computer and Information Sciences Department. 2016;8:1–5.
27. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Comput Netw. 2015;56:133–51.
28. Arbia RiahiSfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, "A Roadmap for Security Challenges in Internet of Things", *vol. 12*, pp. 15–21, 2017.
29. Kim Thuat Nguyen. Maryline Laurent, NouhaOualha, "Survey on secure communication protocols for the Internet of Things." Ad Hoc Network. 2015;7:5–15.
30. Linthicum D. Responsive Data Architecture for the Internet of Things. IEEE Comput. 2016;49(10):72–5.
31. Dongsik Jo and Gerard Jounghyun Kim. ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere. IEEE Trans Consum Electron. 2016;62(3):334–40.
32. Xinlie Wang, Jianqing Zhang, Eve. M. Schooler, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT", Communications (ICC), 2014 *IEEE International Conference, vol. 19*, issue 3, pp. 56–88, 2014.
33. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): A vision, architectural elements, and future directions. Elsevier Future Generation Computer System. 2013;29(4):23–66.
34. Mohamed Abomhara and Geir M. Koien, "Security and Privacy in the Internet of Things Current Status and Open Issues", *In Privacy and Security in Mobile Systems (PRISMS), pages 1–8. IEEE, vol. 7*, issue 6, pp. 18–3, 2014.
35. Ahmad W Atamli and Andrew Martin, "Threat-Based Security Analysis for the Internet of Things", *In Secure Internet of Things (SIoT), vol. 4*, issue 1, pages 35–43, 2014.
36. Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Comput Netw. 2010;8(6):18–30.
37. Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)", *In International Conference*

on Network Security & Applications (CNSA), volume 89, pages 420–429. Springer Berlin Heidelberg, vol. 4, issue 1, pp. 25–30, 2010.

38. Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi, "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples", *2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012 - Digital Proceedings, vol. 11*, issue 6, pp. 13–30, 2012.
39. Jan Camenisch and Els Van Herreweghen, "Design and implementation of the idemix anonymous credential system", In Vijayalakshmi Atluri, editor, *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA*, November 18–22, 2002, pages 21–30, ACM, 2002.
40. Yogeesh Seralathan, Tae (Tom) Oh , Suyash Jadhav, Jonathan Myers, Jaehoon (Paul) Jeong+, Young Ho Kim, and JeongNeyo Kim, "IoT Security Vulnerability: A Case Study of a Web Camera", *International Conference on Advanced Communications Technology(ICACT), IEEE, vol. 13*, issue 9, pp. 16–30, 2018.
41. Vorakulpipat C, Rattanalerdnusorn E, Thaenkaew P. Hoang Dang Hai, "Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study." International Conference on Advanced Communications Technology (ICACT). 2018;7(4):14–33.
42. Jesus Pacheco, Daniela Ibarra, Ashamsa Vijay, Salim Hariri, "IoT Security Framework for Smart Water System", *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications, IEEE, vol. 9*, issue 3, pp. 11–30, 2017.
43. Se-Ra Oh, Kim Y-G. Development of IoT Security Component for Interoperability. IEEE. 2017;12(4):67–89.
44. U. M. Mbanaso, G. A. Chukwudebe, "Requirement Analysis of IoT Security in Distributed Systems", 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), *IEEE, vol. 5*, issue 7, pp. 20–30, 2017.
45. Zhang Y, Li Xu, Dong Q, Wang J, Blauw D, Sylvester D. Recryptor: A Reconfigurable Cryptographic Cortex-M0 Processor with In-Memory and Near-Memory Computing for IoT Security. IEEE J Solid-State Circuits. 2018;9(3):25–56.
46. Ibrahim R. Waz, Mohamed Ali Sobh, Ayman M. Bahaa-Eldin, "Internet of Things (IoT) Security Platforms", *IEEE, vol. 6*, issue 4, pp. 5–19, 2017.
47. Israr Ahmed1, Saleel A. P2, Babak Beheshti3, Zahoor Ali Khan4, Imtiaz Ahmad, "Security in the Internet of Things (IoT)", *The Fourth HCT Information Technology Trends (ITT 2017), Dubai, UAE, vol. 9*, issue 5, pp. 9–30, 2017.
48. Ling Z, Liu K, Yiling Xu. YierJin, Xinwen Fu, "An End-to-End View of IoT Security and Privacy." IEEE. 2017;7(4):22–30.
49. Swapnil Naik, VikasMaral, "Cyber Security – IoT", 2017 *2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT)*, May 19–20, vol. 12, issue 4, pp. 66–78, 2017.
50. Aanchal Punia, Dr. Daya Gupta, Shruti Jaiswal, "A Perspective on Available Security Techniques in IoT", 2017 *2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT)*, May 19–20, vol. 9, issue 6, pp. 25–30, 2017.
51. Daud M, Khan Q, Saleem Y. A Study of Key Technologies for IoT and associated Security Challenges. IEEE. 2017;9(4):22–46.
52. Dou C, Chen W-H, Chen Y-J, Lin H-T, Lin W-Y, Ho M-S, Chang M-F. Challenges of Emerging Memory and Memristor Based Circuits: Nonvolatile Logics, IoT Security, Deep Learning and Neuromorphic Computing. IEEE. 2017;9(1):25–44.
53. Mohamed Tahar Hammi. Erwan Livolant, Patrick Bellot, Ahmed Serhrouchni, Pascale Minet, "A Lightweight IoT Security Protocol." IEEE. 2017;11(6):15–30.
54. Parul Datta, Bhisham Sharma, "A Survey on IoT Architectures, Protocols, Security and Smart City based Applications", 8th *ICCCNT, vol. 9*, issue 4, pp. 25–5, 2017.
55. Chinmaya Mahapatra, Zhengguo Sheng and Victor C.M. Leung, "Energy-efficient and Distributed Data-aware Clustering Protocol for the Internet-of-Things," *IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), volume 4*, issue 33, pp- 643–651, 2016.
56. Mario FRUSTACI, Pasquale PACE, Gianluca ALOI, Giancarlo FORTINO, "Evaluating critical security issues of the IoT world: Present and Future challenges", *IEEE, vol. 8*, issue 4, pp. 25–45, 2017.
57. Kaneko K, Ban Y, Okamura K. "Effectiveness of Experiential Learning for Keeping Knowledge Retention in IoT Security Education", 2017 6th IIAI International Congress on Advanced Applied Informatics. IEEE. 2017;6(4):25–34.
58. Chen Chen, Honghui Zhao, Tie Qiu, Mingcheng Hu, Hui Han, Zhiyuan Ren, "An efficient power saving polling scheme in the internet of energy", *Journal of Network and Computer Applications*, 48–61, 2017.
59. Mian Muhammad Ahemd, Munam Ali Shah, Abdul Wahid, "IoT Security: A Layered Approach for Attacks & Defenses", 2017 International Conference on Communication Technologies, *IEEE, vol. 19*, issue 7, pp. 14–30, 2017.
60. Deogirikar J, Vidhate A. "Security Attacks in IoT: A Survey", International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud). IEEE. 2017;5(2):15–30.
61. Liu X, Huang L, Ravichandran K, Sánchez-Sinencio E. A Highly Efficient Reconfigurable Charge Pump Energy Harvester with Wide Harvesting Range and Two-Dimensional MPPT for Internet of Things. IEEE J Solid-State Circuits. 2016;9(3):552–62.
62. Mukrimah Nawir, Amiza Amir, Naimah Yaakob, Ong Bi Lynn, "Internet of Things (IoT): Taxonomy of Security Attacks", 2016 3rd *International Conference on Electronic Design (ICED)*, August 11–12, vol. 9, issue 5, pp. 25–30, 2016.
63. T. Inzerilli, A. M. Vegni, A. Neri, and R. Cusani, "A Location-based Vertical Handover algorithm for limitation of the ping-pong effect", *in Proc. of IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, vol. 14*, no. 7, pp. 108–117, 2008.
64. Yu T, Wang X, Shami A. Recursive Principal Component Analysis based Data Outlier Detection and Sensor Data Aggregation in IoT Systems. IEEE. 2017;11(24):131–8.
65. Lu R, Heung K, Lashkari AH, Ghorbani AA. A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT. IEEE. 2017;15(4):995–1006.
66. L. Dong, G. Wang, "Inads: In-Network Aggregation and Distribution of Lot Data Subscription in Icn", in *Proc. of the IEEE International Conference on Multimedia and Expo Workshops (ICMEW), vol. 16*, no. 55, pp. 436–445, 2017.
67. Bhandari S, Sharma SK, Wang X. Latency Minimization in Wireless IoT Using Prioritized Channel Access and Data Aggregation. IEEE. 2017;27(16):294–308.
68. Thakare US, Borkar SM. Implementation of WSN's Device Addressing, Data Aggregation and Secure Control in IoT Environment. IJEDR. 2017;5(1):618–25.

Authors and Affiliations

Surbhi Bhatia Khan[1] · Ankit Kumar[2] · Arwa Mashat[3] · Dayananda Pruthviraja[4] · Mohammad Khalid Imam Rahmani[5] · Jimson Mathew[6]

✉ Surbhi Bhatia Khan
s.khan138@salford.ac.uk

Ankit Kumar
iiita.ankit@gmail.com

Arwa Mashat
aasmashat@kau.edu.sa

Dayananda Pruthviraja
dayananda.p@manipal.edu

Mohammad Khalid Imam Rahmani
m.rahmani@seu.edu.sa

Jimson Mathew
Jimson@iitp.ac.in

[1] School of Science, Engineering and Environment, University of Salford, Salford, UK

[2] Department of Information Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur, Chhattisgarh, India

[3] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, P. O. Box 344, Rabigh 21911, Saudi Arabia

[4] Department of Information Technology, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal 576104, Karnataka, India

[5] Department of Computer Science, College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia

[6] Department of Computer Science and Engineering, Indian Institute of Technology Patna, Patna, Bihar, India