Journal of the Maharaja Sayajirao University of Baroda
ISSN: 0025-0422

LOAD BALANCING OPTIMIZATION FORECAST ANALYSIS IN WIRELESS SENSOR NETWORKS USING NETWORK ENERGY EFFICIENT PROTOCOL

Dr. R. Jayaprakash, Assistant Professor, Department of Computer Science, NGM College, Pollachi, Tamil Nadu, India- jpinfosoft@gmail.com

ABSTRACT: The wireless sensor network (WSN) has recently received a lot of interest. One of the most critical and difficulties in Wireless Sensor Networks (WSNs) is lowering energy consumption in order to lengthen the life of the networks. The primary challenges in creating and deploying battery-powered wireless sensor nodes are energy constraints and related concerns. This study makes a contribution by proposing a power-efficient load balancing approach based on the proposed prediction model for extending the life of wireless infrastructure. Significant work was carried out to determine the forecast error rate and energy usage. The findings indicated that the suggested approach greatly lowers the error rate and significantly increases the wireless sensor network's lifetime. Furthermore, by minimizing energy usage, load balancing can help extend the life of a sensor network. Network scalability can also be improved by load balancing via clustering. The lifespan and dependability of a wireless sensor network can be extended by using nodes with varied power levels. We examine how future planned load balancing solutions might be improved. The reader will be able to use this study as a starting point for further research into load balancing strategies for wireless sensor networks.
Keywords: Base station, Clustering, Cluster head, Load balancing, Power.

I. INTRODUCTION

A WSN (Wireless Sensor Network) is a collection of sensor devices at a physical place that are connected via wireless links. Wireless sensor networks might be used for a variety of purposes, including detecting and acquiring data from physical world that people are unable to access. As a result, under such circumstances, sensor nodes must live for as long as possible in the problematic zone. Wireless sensor networks have a number of issues. The main problem is maximizing network dependability and longevity (WSN), which is heavily focused on sizable convergent and energy efficiency. Energy-efficient techniques can be used to protect important sensor-node resources. This is one of the most pressing issues facing WSNs, and it has a significant impact on the network's existence. However there are a variety of WSN protocols, clustering-based hierarchical routing methods are given higher priority due to their increased scalability. Sensors are now battery-powered, which limits space available and is difficult to modify with most circumstances. The constraints of battery and node power systems show that energy is a major concern when using WSNs for various purposes [1].

Much research has been done in recent years to address the important concerns of energy limits. A typical strategy is used to cluster the nodes in periodic data collection applications. In this strategy, every cluster selects a leader node known as the cluster head (CH) network, but all associated nodes communicate their sensed data to the associated CH node. The data is aggregated by the CH nodes and sent directly to the BS or via other nodes using a multi-hop communication technique. The major goal of this strategy is to reduce the amount of messages that must be transmitted to the BS by using local aggregation, as well as to reduce long-distance transmission to save energy [2].By splitting sensor nodes as cluster heads, energy consumption via a wireless network may be reduced (CHs). For data collection and transmission to BS, these CHs demand greater energy. WSN uses a variety of routing techniques to allocate energy consumption to CHs. CH is also in charge of verifying which nodes are permitted to join a cluster and connect with a network. Utilizing additional resources may have a detrimental influence on a network's longevity. As a result, in order to establish encrypted connection across nodes, WSN must consume the least amount of power possible [3].

Whenever networks claims to offer secure communications, it clearly consumes energy by ensuring the nodes' validity, privacy, and stability. As a result, in contexts demanding high security, optimum energy efficiency is critical for optimizing lifetime of the network and improving safety. There are essentially two vital steps in clustering processes. Few nodes are classified as CHs during first stage

and form diverse clusters, whereas data collection and transmission are frequently correlated in the second stage. Each cluster's individual nodes provide their sensory data to their respective CHs, which process this further before sending it to the sink node. CHs waste more energy than conventional nodes since they are accountable for multiple activities [4]. Furthermore, most of the cluster phase picks the CH at random, without taking into account critical characteristics, which might lead to the CH selecting an inadequate node. Other grouping systems are based on a centralized system that might affect the network's sustainability by requiring stations to communicate their parameters, such as resources and the number of neighbors, to the base station, which increases the network inefficiency. As a result, this paper suggests a clustering system based on a distributed approach for energy efficiency, higher throughput, and bandwidth allocation.

Multiple integrated wireless sensor networks (WSNs), in which sensors collect data from real-world settings, have generated a number of current smart infrastructures. The minimal energy available for each sensor, where battery is the power source, is a significant barrier in field. Such a challenge has a direct impact on the lifespan of such integrated networks and, as a result, their long-term viability. In a smart environment, there are several interconnected and heterogeneous WSNs that are controlled by a cloud infrastructure. Real-time processing, in which cloud services reply to queries promptly, is a critical activity on this platform. However, integrating various networks contributed to the difficulty of keeping power usage under check (load balancing). When sensor nodes have varied energy utilities and power consumption techniques, the issue occurs. For example, if some sensors lose power, the system may be unable to deliver the necessary functionality. As a result, in such systems, where sensory nodes are dispersed across a vast region, stability are important considerations.

II. LITERATURE SURVEY

Many energy-aware techniques to tackling the problem of limited energy in WSNs have been presented. Prediction-based energy-efficient strategies are grouped into three categories, based on (1) database level, such as minimizing information creation, communication, and analysis; (2) routing algorithms, such as identifying the simplest pathways; and (3) burden minimization. The remaining of this part displays and contrasts just data-level strategies, as our contribution concentrates on techniques.

Because the problem of distributing energy load is multiclass (depending on the kind of sensor, time, location, and context), generalizing the logistic regression method to forecast discrete results (sensor IDs) would aid in the creation of the load balancing approach. To put it another way, the main goal of this study is to propose a prediction technique that predicts the best set of sensors that can handle a specific task for dynamic load balancing, where a job is assigned to one or more sensors after ensuring that the chosen nodes will achieve network coverage, as a way of extending the battery life of integrated Wireless ad hoc networks [5].Recent studies focus on establishing efficient data communication systems to minimize the number of transmitting messages and, as a result, the pace of energy demand. The quantity of energy necessary for computing is specifically defined as the amount of electrical power required by a node to execute a set of instructions. In [6] Although computing is a substantial source of energy, past research on comparable applications has shown that this element may be overlooked because the amount of energy needed for data transmission is usually much more than that necessary for calculation.

The semi-ring theory was used by Qin et al. [7] to provide a trust sensor secure routing protocol that took into account trust degree and quality of service criteria. To provide efficient and reliable data transfer, routing protocol is used to the secure routing method. At the same time, routing protocol maintenance procedure is employed to assure data transfer security. The sensor node's trusted degrees was determined based on these features, and then the route's trust degree was computed, and the network's trust measure that assesses was built to determine the route from the source to the destination node..

A secure hierarchy and position routing mechanism was presented by Sarma et al. [8]. The position routing mechanism concept is framed by a mix of symmetric and asymmetric cryptographic techniques. The device area was organized into logically regions, with nodes serving various tasks

such as regular sensor node, cluster head, and gateway node in each cluster. The nodes have utilized various key for message encryption and decryption at different phases. With knowledge of numerous threats such as impersonation, node insertion, interruption of service, node capture, reply, and prediction attempt, the position routing mechanism has enhanced energy efficiency. Various routing protocols have been developed to address security issues and protect data from unwanted intrusions.

Sensor nodes in a big sensor network can be clustered into tiny clusters. Each cluster has a cluster head that is in charge of coordinating the cluster's nodes. By requiring the cluster head to collect data from the cluster's nodes and transfer it to the base station, the cluster design can extend the sensor network's lifespan [9]. A cluster creation technique is required to split a randomly distributed sensor network into clusters. It's also a good idea to choose the cluster heads. In this procedure, two ways are used: the head first method and the clustering early method. The cluster head is chosen first in the leader first strategy, and then the cluster is constructed. The network is constructed first, and then the cluster head is chosen in the grouping next technique [10].

The rest of this paper is laid out as follows. The technique for a hierarchical protocol that is energy efficient is described in Section 3. The numerical findings and comments are provided, Performance Study in Section 4, while the conclusion observations are offered in Section 5.

III. PROPOSED APPROACH

The suggested method considers a network model with varied energy levels and computing power among the sensor nodes. A number of high-performance computer nodes have been placed in close proximity to one another. The nodes with the highest starting energy and processing power are chosen. Because of their position, several nodes from the set are chosen as cluster heads (CH). To build a cluster, each CH determines its communication range in terms of power level. Certain nodes in the CH range with equivalent energy and computing power are requested to rest, and information about those nodes is kept with the CH.

To join the network, each given by the national a greeting request message to all nodes inside its own transmission ranges. This procedure will be followed for every CH. The detected data will be sent to the CH by all neighbor nodes. The CH will either deliver the gathered information directly to the Base Station or through an external CH. Whenever the CH's residual energy reaches the TL barrier, the CH would reactivate a few of the resting node and making it its CH. The knowledge given the recent CH will be forwarded to all active nodes, as well as other CH. The former CH will now function as a generic sensor network. This part lays out all of the concepts and the model, before going into the proposed scheme in depth.

3.1 Representation of Networks

The network lifespan is one of the most critical performance parameters in WSN. As a result, the nodes on this direction could rapidly run out of resources, and would choose neighbors who can carry the burden and stability pertaining from their own and neighbor's power scenarios, as well as have a dynamic array of neighbor energy, which can prevent a new point from running out of power generation. After construction, nodes are scattered in an area and fixed.

The base station (BS) is stationary and located outside of the network's coverage region. Nodes have no knowledge of their position and are not integrated with a global positioning system. The round sensed data are acquired and sent to the BS after local aggregation in a network application, which is a periodical intelligence gathering. Based on the intensity of the receiving signal from the node, every node may determine its range to some other node or the BS. The BS has no limitations in terms of energy processing or storage.

3.2 Energy efficiency models

First, a uniform interfering value has been maintained across the cells, with the interfered level being estimated in relation to the actual load demand. The suggested model includes an interfering evaluation to calculate the interfering range and compute the Signal strength in the cell. The interfering range is a relationship between data transmitted either with or without interference.

The power needed to transport an R bit message to a distance of l is:

$$P_{dx(l)} = (P_{ox} + \mathcal{E}_d l^{5)}. R \qquad l \leq \beta \qquad (1)$$

P_{ox} is the power consumption of the wireless circuitry, while ε_d and f are the multipath propagation network.

Mode of acquiring as below is the energy usage in this mode:

$$\mathbf{P_r = P_{ox} . R} \quad (2)$$

In processing mode, the microcomputer is expected to spend power simply for collecting detected data as follows:

$$\mathbf{P_{ps} = P_{dga} . n. R} \quad (3)$$

The volume of data packets is n, and the data gathering power is $\mathbf{P_{dga}}$.

3.3 Protocol Explanation and Cluster Knowledge

Every round in this procedure is divided into two parts: the set up stage and the steady flow stage. In the first phase, the cluster and cluster heads are chosen, and in the second phase, data is collected based on the layout set in the previous cluster formation, so that individual nodes have sent their information directly to the appointed source node, and cluster heads, after aggregating the data, send it to the BS. We'll go through how the protocol chooses cluster heads and forms clusters in the sections that follow.

Before the next round, all hubs evaluate their range to the BS in early stages.

To choose cluster - head, the presented algorithm selects certain possibilities from high-level energy node related to energy information compiled by cluster heads during the provirus round. In order to preserve reduced nodes, nodes whose power is less than a threshold (P_{th}) are effectively not candidates. This threshold varies by node, however it is constant for every base station during operation of the network:

$$\mathbf{P_{th} = \left(\frac{M}{N}\right). P_{ox} . (1+\chi) + P_{d(l(i,BS))}. R_{data}} \quad (4)$$

while i is the nodes ID, N is the required cluster count, is the protocols specification, R_{data} is the packet data length, and $l_{(i,BS)}$ is the length among node I and the Base Station.

Operators send out a message termed ch-message including their I-D, range to the BS, and activates after finding cluster heads. Now, every node forwards that has received some or all of the ch-message packets chooses its cluster head to transmit sensory information to, as shown below.

Then every member node forwards a merge message to its cluster head, including its I-D, cluster head I-D, and remaining power. Every cluster head recognizes its nodes, and all cluster-heads collaboratively for the use in the next round, informing all nodes. Following such approach, each cluster-head sends a schedule-message message to all individuals informing them of the time slot numbers to which they should submit their information, and the channel access is dependent on the protocol.

The part of this section is now complete, and the set point stage has begun.

IV. SIMULATION OUTCOMES

To assess the recommended protocol energy savings, it is simulated and the outcomes to other efficient energy protocols, the LEACH protocol. The MATLAB tool is used to simulate all methods in this effort. Different lifespan concepts have been proposed by the authors. This is entirely dependent on the network application, while some studies have defined longevity in terms of protocol analysis efficiency. In this study, the network lifespan is defined as the time it takes for the first node to die in a round. As a result, in order to extend long life, a protocol should take into account both energy usage and load balancing, particularly across nodes in different regions of the networks.

Table: 1. Notations and Parameters

Parameter specification	Value of parameter
Area	(0,0)~(120,120)
Position of BS	(60,170)
M	120
$P_{initial}$	5J
P_{ox}	60 n-J/bit

ε_d	10 p-J/bit/m ^{2}
β	75
P_{dga}	5 n-J/bit/ sig
Packet size of data	3000 bits
Size of Control Packet	150 bits

In addition, a large number of cluster-heads increases the amount of data packets that must be delivered to the BS, which increases power usage, especially in circumstances when the BS is located far away. Intra cluster power usage is raised throughout the network in a few circumstances.

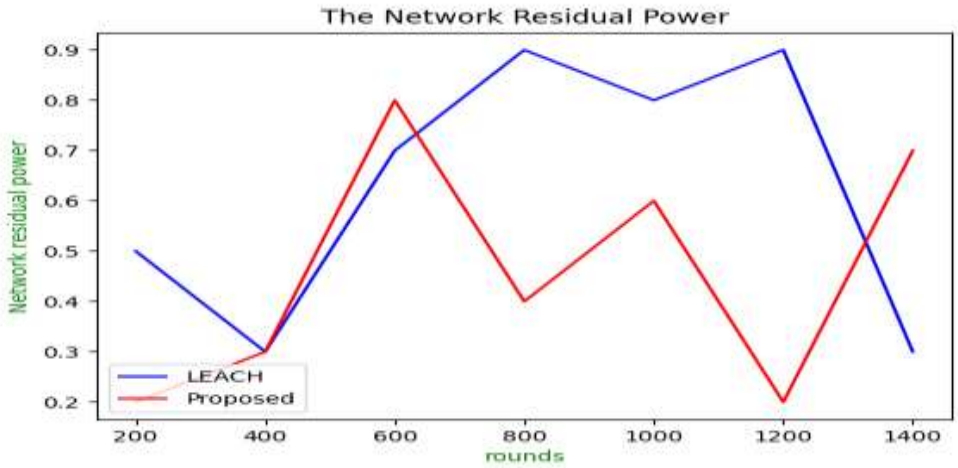

Fig. 1: The Residual Power in the Networks

V. CONCLUSION

This study revealed a decentralized power protocol that takes into account the network CH node count variability and CH dispersal. The proposal reduces total power usage while also improving load balance, according to simulation results. In comparison to the LEACH protocols, the suggested protocol enhanced functional network lifespan by 17%.

References

1. K. Sohrabi, D. Minoli, and T. Znati, "Wireless sensor networks, technology, protocols, and applications", John Wiley, 2017.
2. G. Anastasati, M. Conti, M. D. Francesco, and A. Pasarella, "Energy conservation in in wireless sensor networks: a suevey", Ad Hoc Net. , vol. 6, pp. 537-568, 2019.
3. El-Saadawy M and Shaaban E. Enhancing S-LEACH security for wireless sensor networks. In: Proceedings of the IEEE international conference on electro/ information technology (EIT), Indianapolis, IN, 6-8 May 2012, pp. 1-6. New York: IEEE.
4. M. M. Afsariand M. H. Tayarani-N, "Clustering in sensor networks: A literature survey," J.Netw. Comput. Appl. vol.46, pp. 198–226, 2014.
5. Ahmed, A., Bakar, K., Channa, M., et al.: 'A secure routing protocol with trust and energy awareness for wireless sensor network', Mobile Netw. Appl., 2016, 21, (2), pp. 272–285.
6. Razaque, A., Rizvi, S.: 'Secure data aggregation using access control and authentication for wireless sensor networks', Comput. Secur., 2017, 70, pp. 532–545.
7. Qin, D., Yang, S., Jia, S., et al.: 'Research on trust sensing based secure routing mechanism for wireless sensor network', IEEE Access, 2017, 5, pp. 9599–9609.
8. Sarma, H., Kar, A., Mall, R.: 'A hierarchical and role based secure routing protocol for mobile wireless sensor networks', Wirel. Pers. Commun., 2016, 90, (3), pp. 1067–1103.
9. Nurhayati, S.H.Choi & K.O. Lee, "A cluster Based Energy Efficient Location Routing Protocol in Wireless Sensor Networks", International Journal of Computers and Communications, Volume 5, Issue 2, 2011.
10. G. Anastasati, M. Conti, M. D. Francesco, and A. Pasarella, "Energy conservation in in wireless sensor networks: a survey", Ad Hoc Net. , vol. 6, pp. 537-568, 2017.