QoS analysis of Leach Routing Protocol in Sensor Network

Ritika Bisht [1], Gunjan Negi [2]
M. Tech. Scholar [1], Asst. Prof. [2]
Guru Ram Das Institute Of Management And Technology [1,2]
Rajpur Road Dehradun Uttarakhand-248001 [1,2]

Abstract - Wireless Sensor Nodes generally have less battery life and less memory. Because of that constraint, we need a strong algorithm that allows us to reduce energy consumption as well low loss of packets. Throughout transmission of the data the energy is used for transmitting the packets. Part of the energy is utilized for data processing. We compare the Energy Consumption and Packet Loss Analysis of LEACH Routing Protocol on WSN over DTN. So we must use short-distance routing and data compression to reduce the power consumption. Using connected wireless sensor nodes a wireless sensor network is created, so each node is very compact and capable of detecting, storing, processing and communicating with other nodes within the environment. Good adaptability, good tolerance of faults and broad perception are the key advantages. Such functions enable the extension of wireless sensor networks to various applications, such as environmental monitoring, home care, medical care, and monitoring of battlefields. Recently WSNs have become a vital study area. Through wireless sensor networks more energy is used during the contact cycle between the sensor nodes. Prior the DTN do work as same as the WSN work on distributed platform. But in the term of efficiency and loss it find better ultimately have selective choice of WSN over the DTN.

Keywords- QoS, LEACH, Sensor Network, DTN

1. Introduction

A protocol is the process of selecting the correct path from one source to a destination. The process will face particular difficulties when selecting a route, depending on the type of network, channel features, and performance indicators. Data transmitted by sensors via a Wireless Network (WSN) sensor node is typically transmitted to a channel used to link the sensor network to other networks (maybe the Internet), where information is processed, evaluated, and action taken. The sensor network is very small, the gap between the base station and the sensor node is so near that they can interact directly, this is a single hop communication, but the spread is needed in most WSN implementations Hundreds of nodes, since most nodes are far from each other. The receiver node (gate) is very small, and they cannot interact directly with the source, and this approach needs a lot of communication. Single-hop contact is often referred to as direct contact, and indirect communication is named in other hops.

The sensor node not only constructs and transmits its own artifacts in multi-hop communication, but also serves as a conduit from other sensor nodes into the base station. The process of finding the correct path from the source node to the destination point is called the route, which is the network layer's principal responsibility.

1.1 Wireless Sensor Network

Wireless sensor networks are networks which coordinate themselves. This has a tiny wireless sensor device, called a sensor module, positioned under conditions of physiology or the climate. Physical parameters such as vibration, sound, temperature, and humidity are also calculated. These sensors are used in huge numbers or in thousands and are incorporated.

Build an wireless network which can report on the keys to collect data (base station). Wireless sensor networks provide a range of tools, including position control, land detection, safety monitoring, military survival slums, and mapping. When we talk about power, computing, memory and limited communication capabilities, however, wireless sensor networks will be resource-limited.

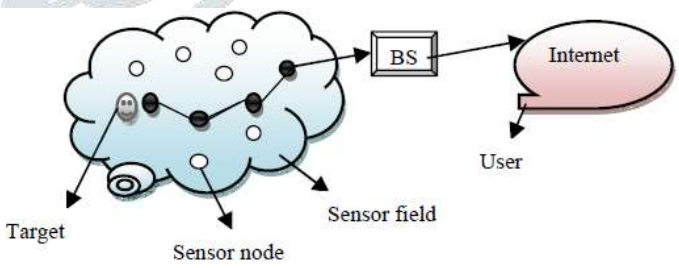

Figure 1: Architecture of the Sensor network

All sensor nodes in the network of wireless sensors connect with others or through unified sensor nodes. The sensor node creates data according to their sensing system's visual influence, and transmits a heart-shaped data envelope to the base station (receiver). The better solution is to provide a few locations and transmit data to the base station. Such regions are classified as aggregator nodes, and the method is called wireless sensor network data aggregation.

It comprises a small range of naturally distributed sensors inside a specified (usually defined) internal or external

environment. WSN aims at collecting natural data, so node system location can be a priori or anonymous. The location of the network can communicate physically or logically with all the devices. Depending on the application, that communication defines topology. Two WSNs with the same topology can exist, for example (mesh, star, etc.). That isn't valid with all programs however. Logical topology is defined primarily by the logical roles of the surfaces (functions, etc.). This could be temporary or legislation dependent (self-organizing, capturing, and monitoring pheromones, etc.). Strategy is established, based on the network's capital.

Medium-architecture technology is ideal for networks which are primarily focused on a single computer. This system is liable in this case for storing, organizing and handling the reasonable knowledge activities. It also transmits these data to the host area (Figure 1). The key benefits of this method are: I Long term approaches will accomplish effective energy production (see section 5). (Ii) Allow network roaming; (Iii) Simplify an overview of the network. (Iv) Providing contextual information allows for better program design (node decoding, device recognition, etc.).

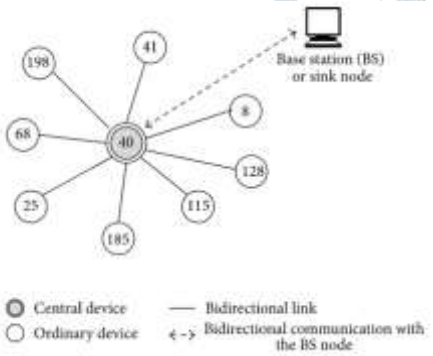

Figure 2: Centralized strategy.

Self-organization is one of the most shared technologies in recent years. The sensory networks using this technique can induce an emerging process in which nodes interact in secret and automatically connect. The goal is to complete tasks beyond the capacity of a single node. Examples of these strategies are found in the environment (insect communities, natural cells, bird populations, ethics, etc.

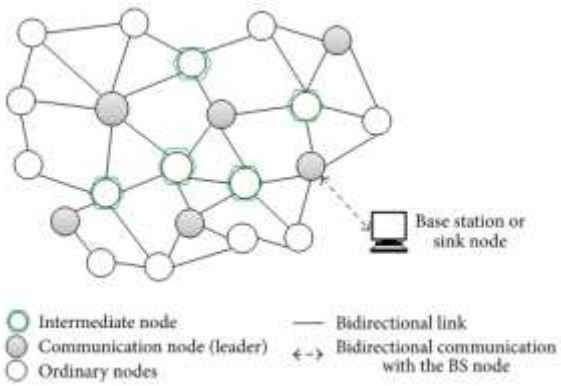

Figure 1: Self-organization strategy.

It is a topic explored in the next segment. This indicates the approach we have suggested for the classification. This integrated or distributed system present the scenario of WSN network as a self-organized nodes.

The field of wireless network and mobile computing is considered to be rapidly developing. Most importantly wireless networks are cost-effective. When we equate wireless networks with wired networks, we can gain more benefits from wireless networks because they can be expanded easily and implemented effectively. Wireless networks are especially cost-effective. The sensor node is a low-power device with integrated detection feature, sensor nodes provide limited processing and wireless communication capability.

We are looking for secure routing for tasks of data collection which is one of WSN's most basic functions. With the support of other intermediate nodes, sensor nodes send their collected data to remote base stations for data collection tasks. Although there may be multiple base stations, our routing method will not be affected by the number of base stations; to simplify our discussion we assume there is only one base station. The opponent will forge the legal node identity by copying the node's outgoing routing data packet, and forge the identification data packet remotely via the wormhole. Because the nodes in WSN usually rely only on the received data packets to understand the sender's identity, replication of the routing data packets allows malicious nodes to deceive that valid node's identity. After "stealing" the legal identity the malicious node will redirect network traffic. For instance, you can discard the received packet, forward the packet to another node that should not be in the routing path, or even form a transmission loop, allowing the packet to pass indefinitely between multiple malicious nodes. This is also impossible to learn that even with overhearing strategies, a node forwards interpreted packets correctly. Receiver attack is another type of attack which can be carried out after a valid identity has been stealed. A malicious node may claim to be a base station in a sink attack by playing all the data packets from an actual base station. Such a fake base station can attract more than half the traffic, thus forming a "black hole."

Another powerful attack type can be used with the same strategy: Sybil attack: by copying the routing details of multiple valid nodes, an intruder can provide multiple identities to the network. If attacked, all these attacks can be launched by the successful node too. WSN's flexibility and the network's aggressiveness further intensify the devastation of these malicious attacks (focusing on repeated route sensitivity technology). Although the versatility of effective data collection is realized in WSN and various applications, the chance of contact between honest nodes and attackers is greatly increased. In comparison, a weak link to the network creates significant difficulties in discriminating between an intruder and a trustworthy node

of intermittent loss. Under some conditions, WSNs with current routing protocols will suffer total destruction without adequate security. Protecting the network from damage is critical to the application's success in emerging detection applications which emerge through WSN.

1.2 Data Accumulation in WSN

This chapter discussed two important factors in this article which affect the output of data integration methods in wireless sensor networks, such as energy storage and latency. Data aggregation is the mechanism by which data packets from different outlets are combined; transmission volumes are that. We can save energy on the network with that method. Latency is a latency correlated with aggregated data from nearby sources and may cause delays to combine aggregated data from distant sources in central locations. This is an aggregation approach that focuses basically on the position of the source on the network, the number of sources and the network findings. When we look at these stuff we're going to look at two forms of source positioning. Event layout for radio and spontaneous configuration for source [14]. The simulation shows us that data aggregation will dramatically increase energy efficiency as resources are spread closely or at random. These benefits are best where there is a huge number of outlets, especially where the outlets are close to each other and not at base station. Using the models it tends to mean that the pause of integration may not be optimal.

1.3 Delay-tolerant Network

A delay-tolerant network is a network intended to run for long periods (such as telecommunications or interstellar telecommunications); in such a situation lengthy periods are inevitable (sometimes in hours or days). Nevertheless, in the non-infectious context, related issues can occur when interference becomes severe, or when network resources are too crowded.

Fault-responsive networks use some of the same systems as are found in tolerant networks, but major variations do occur. Delayed networks require equipment capable of processing massive volumes of data. Such devices will be able to tolerate extended power outages and reboots of the network. It will also be easily available at any time. Suitable hardware for this purpose requires fast storage memory and hard drives. To ensure accurate and efficient archiving, the material contained in such media must be filtered and prioritized by the Program.

Traffic can be divided into three forms for a delay-tolerant network: fast, regular, and batch, so as to decrease priority. Emergency data packets are often transferred, reassembled, and validated from a given source to a given source before any other data form. Upon effectively combining all emergency data packets to their desired target, normal traffic would be sent out. This is only when all data packets in certain types from the same source are effectively transmitted and reassembled and bound to the same place that the key traffic will be handled.

1.4 Energy consumption in WSN

It turns out that the main power consumption is due to their radio transmission and receiver system in each sensor network. In WSN the method of data transmission requires a lot of resources. Reducing overhead connectivity would reduce the electricity usage. Managing the method and network levels of MAC setup, hardware management and device convergence will also aid in energy savings.

1.5 Packet Loss in WSN

Packet loss is a failure when one or more data packets that can't reach their destination are delivered. Loss of a packet lowers the packet's transfer value. Packet loss can be caused by many factors including signal degradation due to duplication ends in the network area. Packs on wireless sensor networks may get lost. This way, hackers can access the data quickly. Identifying lost data packets and anomalous behavior is a much-needed measure of secure transfer. The node will not be able to participate in the transfer, without a certificate.

For power deficient networks, packet distribution is quite critical because it can be converted into a safety measure for the network. Wireless communication opportunities make WSN a viable solution for exploring different, sometimes harsh and inaccessible environments, and will demonstrate great multifaceted communication. Packet transmission works mainly according to the environment, the selected encoding system, and the various distribution circuit features.

2. Methodology

Low Energy Adaptive Cluster Hierarchy Protocol (LEACH) The LEACH Protocol is the first-line agreement which proposes the integration of data. The party route configuration is a landmark. Many layered route processors are protocols built using the LEACH protocol [3] as their basis. So as wireless sensor networks slowly join our lives, learning the LEACH protocol is quite necessary. For the routing protocol the LEACH protocol is a regular proxy. Organized and efficient. The LEACH algorithm takes as unit cycles. Each process is composed of a cluster of clusters and a stable global step. For excessive energy prices to be that, the sustainable state sector will be even longer than the establishment process.

Throughout LEACH the cycle is separated into loops-lengths, where each loop starts with the step of initiation and then the duration of the stable state. The cycle time is a priori set. The LEACH algorithm Implementation is as follows:

• **Broadcast Category:** nodes vote by cluster broadcasting messages in this category to become the new process (r) cluster leader. The Cluster header uses the CSMA MAC

rule to designate a cluster header. After this phase is complete, it depends on head nodes in the current (r) cycle determine the appropriate clusters. Node n selects a random number k for each move, which is between 0 and 1

• **Cluster Setup Phase:** time for each cluster header to decide which cluster and notify the group header to enter the cluster. And any node uses the CSMA MAC protocol to transmit this information to the header of the cluster.

• **Network construct phase:** Cluster head node collects messages from all cluster positions to be implemented. The head node of the cluster establishes a TDMA scheme dependent upon the amount of positions in a cluster. The timetable informs any node where to give it. The software is distributed back to the group's places.

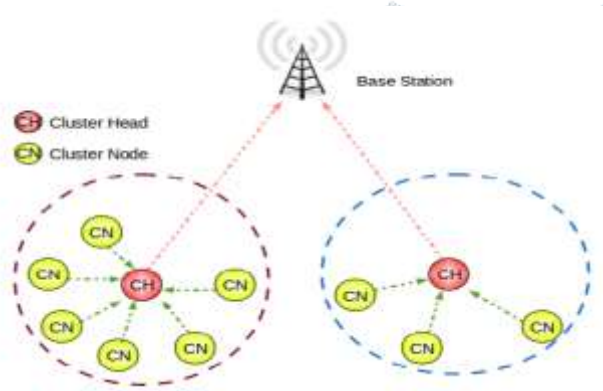

Figure 4: Depiction of Leach Protocol.

• **Data Transfer Phase:** Once the TDMA configuration of the cluster is defined and the community is formed, at the time of the allocated distribution, they begin to transfer personal data to the group leader. This will conduct signal processing operations after submitting all the data obtained by the cluster node to simplify the data into one single signal.

LEACH Agreement references can create problems in a lot of real-time applications. The most popular guess is:

• All locations can send sufficient power to the base station, if necessary.

• Each site can support different MAC protocols so they have enough computing power. Nodes still have data ready for transmission.

• Allow areas near to each other more data-friendly.
. The system becomes unbalanced, if the first node fails.
• Many regions have the same energy at each selection period.

• For every node the region believed to be the community leader uses the same amount of control.

3. Simulation And Result

Despite the growing usage of wireless sensor networks, it is vitally important to conserve the strength of wireless sensor networks. Some of the main difficulties in coordinating wireless sensor networks is power consumption and reliability, as sensor node battery capacity is small, and replacement of sensor nodes is difficult. For certain areas sensor node versatility is very important. To sustain the network life cycle and efficient packet delivery, packet leakage and power usage need to be taken into consideration in the protocol. There are two concepts we discussed in this post-LEACH and LEACH Phone. The usefulness of the LEACH Mobile protocol is more than LEACH in rising the data packet failure and optimizing efficient data packet distribution. Nonetheless, the former absorbs more fuel, due to the additional control kit. Potential analysis in any step of the LEACH Mobile protocol should concentrate on rising energy usage.

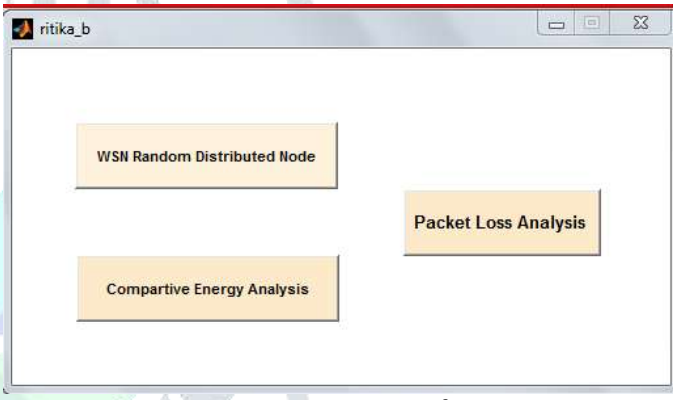

Figure 5: Basic Layout of Project

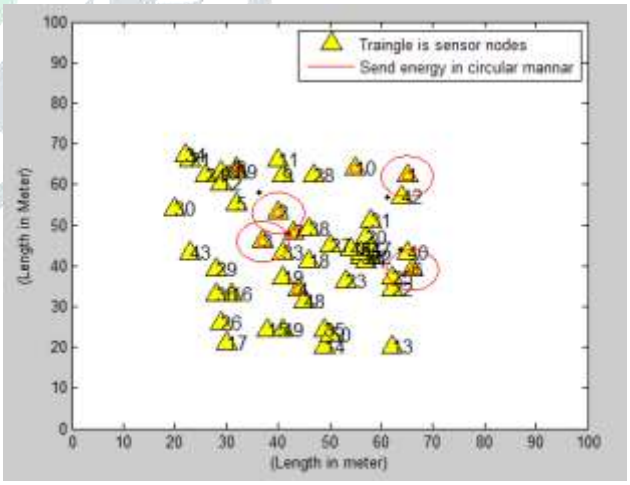

Figure 6: Energy generated in circular manner

```
r3 =
   105

r3 =
   106

r3 =
   107

r3 =
   108

r3 =
   109

r3 =
   110
```

Figure 7: Number of Communication rounds

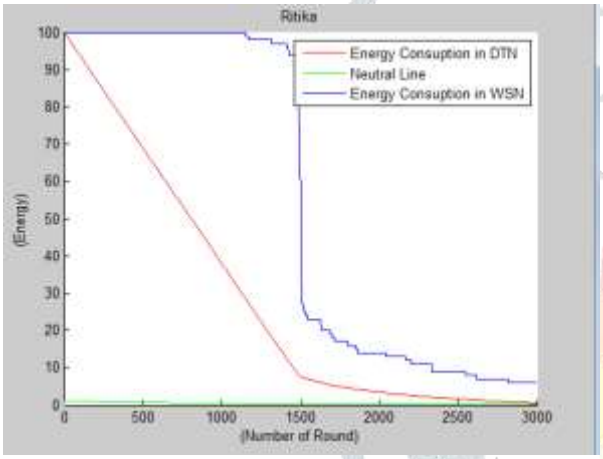

Figure 8: Energy vs. number of rounds of Energy Consumption in DTN, Natural Line, and Energy Consumption in WSN

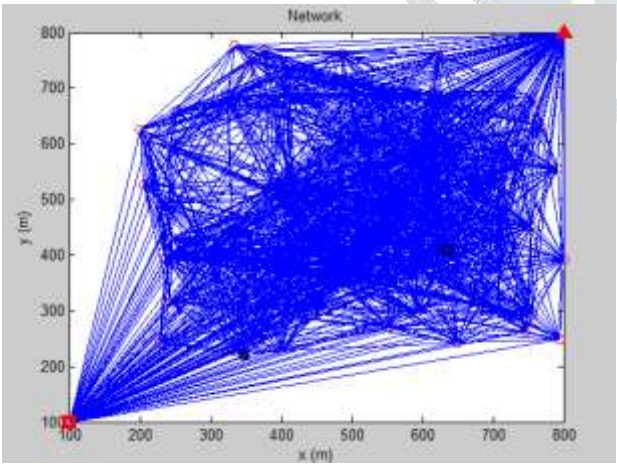

Figure 9: DTN Network

DTN Configuration (0) WSN with AI Based (1) Press = (0/1): 1
Number of packets (max=500)? 200

```
Message Postponded because of low security!
Packet Remaining: 63
Message Postponded because of low security!
Packet Remaining: 63
Packet Remaining: 62
Packet Remaining: 61
Packet Remaining: 60
Packet Remaining: 59
Packet Remaining: 58
Message Postponded because of low security!
Packet Remaining: 58
Message Postponded because of low security!
Packet Remaining: 58
Message Postponded because of low security!
Packet Remaining: 58
Packet Remaining: 57
Message Postponded because of low security!
Packet Remaining: 57
Message Postponded because of low security!
Packet Remaining: 57
Packet Remaining: 56
Packet Remaining: 55
Packet Remaining: 54
Message Postponded because of low security!
Packet Remaining: 54
Message Postponded because of low security!
Packet Remaining: 54
Message Postponded because of low security!
Packet Remaining: 54

stolen_rate =

     0


Total_Time =

  418.8239


Total_Energy =

   1.4912e+03


Packet_Delivery_Rate =

   100
```

Figure 10: Packet loss analysis

The above figure is the screen shot of outcome of packet delivery rate, Energy and time with stolen rate. The final outcome of the proposed technique is been taken out from the simulation.

4. Conclusion And Future Scope

Wireless sensor nodes have less battery life and less power. Because of this limitation, we need a powerful algorithm that helps us reduce energy consumption and low packet loss. Throughout the transmission of data, energy is used to transfer packets. Part of the energy is used for the processing of data. We 're matching LEACH Routing

Protocol's energy consumption and packet loss analysis over DTN. The use short-distance routing and data compression to reduce power consumption. A wireless sensor network is built using linked wireless sensor nodes, such that each node is very small and can track, store , process and interact with other nodes in the area. High adaptability, high fault tolerance and broad vision are main advantages. Such functions enable the expansion of wireless sensor networks to multiple applications such as environmental control, home care , medical care and field control. WSNs have recently been a vital area of study. Wireless sensor networks use more energy between the nodes of the sensor during the touch process. WSN works on the global network previous to the DTN. Yet essentially, in terms of performance and failure, it's better to provide minimal WSN choices than DTN. The result come after the run of simulation of WSN and DTN. The outcome suggest that the as the round of communication increases the energy decreases and the continuous loss of energy has been dissipated. One things is very noticeable in case of WSN over the DTN line the rate of dissipation of energy is quite less in WSN. As per the acceptability of both network set or arrangement of technological need WSN find good. Further Packet loss analysis also has been performed through the MATLAB.

References

1. Salam, T., & Hossen, M. S. (2020). Performance Analysis on Homogeneous LEACH and EAMMH Protocols in Wireless Sensor Network. *Wireless Personal Communications*, 1-34.
2. Patel, P. P., & Jhaveri, R. H. (2020). A Survey of Energy Efficient Schemes in Ad-hoc Networks. *arXiv preprint arXiv:2004.06380*.
3. Prabha, K. L., & Selvan, S. (2018). Energy efficient energy hole repelling (EEEHR) algorithm for delay tolerant wireless sensor network. *Wireless Personal Communications*, *101*(3), 1395-1409.
4. Varshney, S., & Kuma, R. (2018, January). Variants of LEACH routing protocol in WSN: A comparative analysis. In *2018 8th International conference on cloud computing, data science & engineering (confluence)* (pp. 199-204). IEEE.
5. Al-Baz, A., & El-Sayed, A. (2018). A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks. *International journal of communication systems*, *31*(1), e3407
6. Jambli, M. N., Bandan, M. I., Pillay, K. S., & Suhaili, S. M. (2018, November). An Analytical Study of LEACH Routing Protocol for Wireless Sensor Network. In *2018 IEEE Conference on Wireless Sensors (ICWiSe)* (pp. 44-49). IEEE.
7. Shaikh, P. B., & Takale, S. B. (2018). Improved LEACH routing protocol for wireless sensor networks. *International Journal of Advance Research, Ideas And Innovations In Technology*, *4*(4).
8. Rhim, H., Tamine, K., Abassi, R., Sauveron, D., & Guemara, S. (2018). A multi-hop graph-based approach for an energy-efficient routing protocol in wireless sensor networks. *Human-centric Computing and Information Sciences*, *8*(1), 1-21.
9. Khan, M. K., Shiraz, M., Zrar Ghafoor, K., Khan, S., Safaa Sadiq, A., & Ahmed, G. (2018). EE-MRP: Energy-efficient multistage routing protocol for wireless sensor networks. *Wireless Communications and Mobile Computing*, *2018*.
10. Ajaykumar, N., & Sarvagya, M. (2017, September). Secure and energy efficient routing protocol in wireless sensor network: A survey. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 2313-2322). IEEE.
11. Rahmadhani, M. A., Yovita, L. V., & Mayasari, R. (2018, July). Energy Consumption and Packet Loss Analysis of LEACH Routing Protocol on WSN Over DTN. In *2018 4th International Conference on Wireless and Telematics (ICWT)* (pp. 1-5). IEEE.
12. Thapa, R., Singh, H., & Sharma, A. (2017, July). A comparative analysis of LEACH and SEP using NS2. In *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
13. Majid, A., Azam, I., Waheed, A., Zain-ul-Abidin, M., Hafeez, T., Khan, Z. A., & Javaid, N. (2016, March). An energy efficient and balanced energy consumption cluster based routing protocol for underwater wireless sensor networks. In *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)* (pp. 324-333). IEEE.
14. Rahama, M. T., Hossen, M., & Rahman, M. M. (2016, September). A routing protocol for improving energy efficiency in wireless sensor networks. In *2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)* (pp. 1-6). IEEE.
15. Julie, E. G., Tamilselvi, S., & Robinson, Y. H. (2016). Performance analysis of energy efficient virtual back bone path based cluster routing protocol for WSN. *Wireless Personal Communications*, *91*(3), 1171-1189.
16. Li, H., & Liu, J. (2016). Double cluster based energy efficient routing protocol for wireless sensor network. *International Journal of Wireless Information Networks*, *23*(1), 40-48.
17. Dhand, G., & Tyagi, S. S. (2019). SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks. *Wireless Personal Communications*, *105*(1), 17-35.
18. Selvadivya, E., & Priyadarshini, G. (2011). Proficient cluster-based routing protocol using EBSA And LEACH approaches. *Int. J. Comp. Tech. Appl*, *2*(2), 295-299.

19. TazirulIlm, S., & Bordoloi, D. (2015). Resource Constraint Estimation using Performance Metric with respect to LEACH Protocol in WSN. *Resource*, *3*(11).
20. Medjiah, S., & Ahmed, T. (2011, June). Orion routing protocol for delay tolerant networks. In *2011 IEEE international conference on communications (ICC)* (pp. 1-6). IEEE.
21. Zhenyu, L. I. (2014). An Analysis of Ad Hoc Routing Protocols Using ns2 simulations. *Journal of Network New Media*, (4), 14.
22. Tambat, P. M., & Dixit, A. M. (2015, February). Energy Efficient Scheme for Wireless Sensor Networks. In *646 IJRITCC* (Vol. 3, No. 2, pp. 646-653).
23. Razaque, A., Abdulgader, M., Joshi, C., Amsaad, F., & Chauhan, M. (2016, April). P-LEACH: Energy efficient routing protocol for Wireless Sensor Networks. In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-5). IEEE.
24. Azizi, R. (2016). Consumption of Energy and Routing Protocols in Wireless Sensor Network. *Network Protocols & Algorithms*, *8*(3), 76-87.
25. Patel, R., Pariyani, S., & Ukani, V. (2011). Energy and throughput analysis of hierarchical routing protocol (LEACH) for wireless sensor network. *International Journal of Computer Applications*, *20*(4), 32-36.
26. Yan, J. F., & Liu, Y. L. (2011, September). Improved LEACH routing protocol for large scale wireless sensor networks routing. In *2011 international conference on electronics, communications and control (ICECC)* (pp. 3754-3757). IEEE.
27. Chen, Y., Jiang, L., & Mu, Y. (2019, September). A LEACH-based WSN Energy Balance Routing Algorithm. In *Proceedings of the 2019 the World Symposium on Software Engineering* (pp. 37-41).
28. Shao, L., Yang, J., & Fang, J. (2020). A Distributed Optimization Algorithm for Energy of Wireless Sensor Networks Based on Potential Game. *International Journal of Photoenergy*, *2020*.
29. R, Mahima and K S, Kiruthik Ruba and A, Pushpalatha. (2020). Energy Optimized Data Routing Using PSO in WSN. *IJETIE, 6(3)*, 106-115.
30. Hebal, S., Louail, L., & Harous, S. (2020). Latency and Energy Optimization Using MAC-Aware Routing for WSNs. *International Journal of Business Data Communications and Networking (IJBDCN)*, *16*(1), 19-27.
31. Carrabs, F., D'Ambrosio, C., & Raiconi, A. (2020). Optimization of sensor battery charging to maximize lifetime in a wireless sensors network. *Optimization Letters*, 1-14.
32. Yadav, A. K., Rajpoot, P., Kumar, P., Dubey, K., Singh, S. H., & Verma, K. R. (2019, January). Multi Parameters Based Heterogeneous Clustering Algorithm for Energy Optimization in WSN. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 587-592). IEEE.
33. Jha, S. K., & Eyong, E. M. (2018). An energy optimization in wireless sensor networks by using genetic algorithm. *Telecommunication Systems*, *67*(1), 113-121.
34. Cao, Y., & Zhang, L. (2018, April). Energy optimization protocol of heterogeneous WSN based on node energy. In *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)* (pp. 495-499). IEEE.
35. Tayeb, S., Mirnabibaboli, M., & Latifi, S. (2018). Cluster Head Energy Optimization in Wireless Sensor Networks. *Software Networking*, *2018*(1), 137-162.
36. Ali, A., Abo-Zahhad, M., & Farrag, M. (2017). Modeling of wireless sensor networks with minimum energy consumption. *Arabian Journal for Science and Engineering*, *42*(7), 2631-2639.