

Secured Routing Energy Efficient Protocol (Sreep)

Research Scholar R.S.Karthik
CMS College of Science and Commerce
Coimbatore, India
karthiksrinivasan16@gmail.com

Dr.M. Nagarajan
KSG College of Arts and Science
Coimbatore, India.
mnaagarajan@gmail.com

Abstract-The routing mechanism in wireless sensor networks (WSNs) is crucial for a variety of monitoring applications, such as those focusing on the environment and traffic. In this section, the comprehensive contributions made to routing in WSN are examined. This study concentrates mainly on the challenges that WSN confronts as well as the various protocols that are employed. The SREEP algorithm is a brand-new proposal for assuring the secure transmission of data packets. The proposed technique reduces energy consumption while preserving a high level of security. The efficacy of the algorithm is assessed based on energy consumption, transmission duration, latency, and throughput.

Keywords- WSN ,Routing, Energy, SPIN, LEACH

I. INTRODUCTION

[11] A wireless sensor network is a group of dispersed nodes which are deployed under various environmental conditions to monitor the physical changes in the environment. Some of the applications of WSN include animal monitoring, environmental monitoring, medical applications, military surveillance and infrastructure maintenance. There are so many challenges to be faced by WSN which includes drop down of energy level in nodes, death of nodes, hardware failure, unable to locate the nodes, scalability of the network, deployment of nodes etc. [1] The routing protocol is a method for determining the optimal path from source to destination for data.

During the route selection procedure, which is dependent on the type of network, channel characteristics, and performance indicators, numerous complications arise. [12] The data perceived by the sensor nodes in a wireless sensor network (WSN) is typically transmitted to the base station, which connects the sensor network to other networks (including the Internet) for collection, processing, and subsequent action. Single-hop communication is utilized in extremely small sensor networks where the base station and nodes (sensor nodes) are near enough to communicate directly.

Nonetheless, in the majority of WSN applications, the coverage area is so expansive that thousands of nodes must be deployed, and this scenario necessitates multi-hop communication because the majority of sensor nodes are so far from the sink node (gateway) that they cannot communicate directly with the base station. Multi-hop communication is also known as indirect communication. A message which is an essential need of a network. [13] In

multi-hop communication, sensor nodes not only generate and transmit their own content, but also serve as a conduit for additional sensor nodes to the base station. Routing is the process of locating an adequate path from a source node to a destination node; it is the network layer's primary responsibility.

II. CHALLENGES IN ROUTING

[1] Designing routing protocols for WSN is relatively challenging due to the numerous characteristics that differentiate them from wireless infrastructure-free networks. There are numerous types of routing challenges in wireless sensor networks. It is virtually impossible to assign a universal identity system to a large number of sensor nodes. Consequently, wireless sensor nodes cannot utilize traditional IP-based protocols. Required is the transmission of observed data from multiple sources to a specific base station. However, this does not occur in standard communication networks. [11] In the majority of cases, the produced data flow is highly redundant. Due to the fact that a high number of sensing nodes can produce identical data during sensing, it is essential that routing protocols take advantage of this redundancy and utilize the available bandwidth and energy as effectively as possible. In addition, wireless nodes are severely limited in terms of transmission energy, bandwidth, storage capacity, and on-board energy. Due to these distinctions, a number of novel routing techniques have been proposed to address routing issues in wireless sensor networks.

III. THE ROUTING PROTOCOLS

[1] How nodes communicate with one another and how information is distributed throughout the network is

governed by routing protocols. WSN routing protocols can be categorized in numerous ways namely node centric routing protocols, data centric routing protocols, source initiated routing protocols and destination initiated routing protocols. Fig. 3.1 and Table 3.1 describe the different categories of routing protocols and its definition.

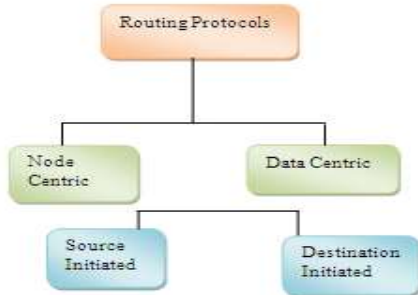


Fig.1. Classification of Routing Protocols.

Table 3.1. Classification of Routing Protocols

Category	Definition	Example
Node Centric	The destination node in node centric protocols is indicated with certain numeric IDs, which is not an expected method of communication in wireless sensor networks.	LEACH
Data Centric	In data centric routing, the sink node queries particular regions to gather data with certain characteristics; hence a naming scheme based on attributes is required to represent the data's qualities.	SPIN
Source-initiated	When the source node has data to share, it advertises it, and the route is generated from the source side to the destination.	SPIN
Destination-initiated	Protocols are referred to as destination-initiated protocols when the destination node generates the path configuration.	LEACH

IV. RELATED WORK

There are numerous extant works and ongoing efforts for the development of routing protocols for WSNs. These protocols are designed with application requirements and network topology in mind. When developing routing protocols for WSNs, it is necessary to consider a number of factors. The energy efficacy of the sensors is the most important factor, as it directly affects the network's lifespan extension. Literature contains a variety of surveys on routing protocols in WSNs; this paper attempts to demonstrate and discuss the differences between these surveys and our work.

The authors of [2] provide an exhaustive analysis of WSN design challenges and techniques (2002). The proposed protocols address all levels of the network hierarchy and specify the physical constraints of sensor nodes. In addition, the prospective applications of sensor networks are emphasized. However, the research does not categorize these routing protocols, and the list of protocols mentioned is not exhaustive given the scope of the study. Our investigation focuses primarily on the energy efficiency of WSNs, as well as the classification of extant routing techniques. In addition, we discuss a variety of new energy-efficient routing protocols and offer guidance on how readers can select the optimal protocol for their network.

[3] The author provides a survey of routing protocols in WSNs. (2004). Based on network structure, it categorizes routing protocols into three groups: flat, hierarchical, and location-based routing systems. Moreover, based on the protocol operation, these routing strategies are classified as multipath-based, query-based, negotiation-based, and QoS-based. It is comprised of 27 routing protocols. In addition, this 2004 survey provides a substantial number of energy-efficient routing protocols that have been developed for WSNs. In addition, it discusses the Routing Challenges and Design Issues that must be considered when employing WSNs. As a result, the energy supply, computing capacity, and bandwidth of the wireless links connecting sensor nodes are limited.

In addition, the authors attempt to emphasize the design tradeoffs between energy and communication overhead savings in certain routing paradigms, as well as the advantages and disadvantages of each routing technique. In contrast, the focus of our research is on energy efficiency issues in WSNs. We provide researchers with information and extensive comparisons regarding energy-efficient techniques. In addition, we expand on Al-initial Karaki's classification in order to improve all proposed publications since 2004 and elucidate which difficulties/operations in each protocol illustrate/enhance energy-efficiency concerns. 24 routing methods for sensor networks are discussed in [4], which classifies

them as data-centric, hierarchical, or location-based (2005). Although routing protocols for WSNs are discussed, energy-efficient policies are not emphasized. In contrast, we focus primarily on energy-efficient routing protocols, addressing the benefits and drawbacks of each protocol to assist readers in choosing the most suitable energy-efficient routing strategy for their network. The authors of [5] present a systematic examination of contemporary cutting-edge algorithms (2007).

In a recent study, they are separated into two categories that account for the broadcast/multicast energy challenge. The authors classify wireless ad hoc network algorithms as either MEB/MEM (minimal energy broadcast/multicast) or MLB/MLM (maximum lifetime broadcast/multicast). The two primary energy-aware criteria that are typically investigated are minimizing the total transmission power consumption of all nodes participating in the multicast session and maximizing the operation duration until the battery of the first node participating in the multicast session runs out. In addition, each network component is believed to be equipped with an omnidirectional antenna that is responsible for signal transmission and reception.

[6] The author adopts a top-down strategy for evaluating multiple WSN applications and features (2008). It divides the problems into the following categories: internal platform and underlying operating system, communication protocol stack, network services, provisioning, and deployment. However, neither the study nor a comprehensive comparison of the energy-efficient routing protocols implemented on WSNs is discussed. Our work is a comprehensive analysis of energy-efficient routing protocols that assists readers in selecting the most suitable protocol for their network. Using the hardware components of a typical sensor node, the authors of [7] conduct a survey of energy consumption (2009). The sensor node is divided into four major components: a sensing subsystem consisting of one or more sensors for data acquisition, a processing subsystem consisting of a microcontroller and memory for local data processing, a radio subsystem consisting of a microcontroller and memory for wireless data communication, and a power supply unit.

In addition, the design and power breakdown are mentioned as strategies for reducing power consumption in wireless sensor networks. They describe the principal strategies for energy conservation in WSNs. This paper describes the characteristics and benefits of the classification of energy conservation schemes. There are three categories of procedures: duty-cycling, data-driven, and mobility-based. The accompanying protocols provide additional details and discussion of this classification. In addition, they comment on the various energy management techniques and emphasize that the radio's energy consumption is significantly greater than that of data sampling or data processing. Numerous

implementations in the actual world, however, have demonstrated that the sensor's power consumption is comparable to, if not greater than, that of the radio. They discover that the sample phase may take a significant amount of time, particularly when compared to the time required for communications, and that the sensor's energy consumption may also be quite high. They also observe a rise in interest in the design of sparse sensor networks. In our work, we focus predominantly on energy-efficient protocols and describe the benefits and drawbacks of each protocol so that readers can select the most efficient routing strategy for their network.

The eighth section discusses WSN design challenges and routing protocol classification (2009). In addition, a few routing protocols are presented based on their characteristics and the methods they employ to increase network lifetime, without delving into detail about each of the listed protocols. In addition, the authors do not provide a precise comparison of the presented techniques. In addition to focusing on energy-efficient protocols in our work, we also address the benefits and drawbacks of each protocol to help readers choose the most suitable energy-efficient routing protocol for their network. The study in [9] discusses the challenges of devising Medium Access Control (MAC) protocols for WSNs that are energy-efficient (2009).

In addition, it specifies a small number of MAC protocols (12 in total) for WSNs, highlighting their advantages and disadvantages whenever feasible. However, neither the study nor a comprehensive comparison of the energy-efficient routing protocols implemented on WSNs is discussed. Our survey concentrates on energy-efficient routing protocols, analyzing the advantages and disadvantages of each protocol to assist readers in selecting the most suitable energy-efficient routing protocol for their network. Several energy-efficient routing strategies for Wireless Multimedia Sensor Networks (WMSN) are presented in (2011). Additionally, the authors highlight the performance considerations associated with each technique.

They clarify the challenges of designing routing protocols for WMSNs, followed by the limitations of existing non-multimedia data transmission mechanisms. In addition, a taxonomy of contemporary routing protocols for WMSNs is provided. This survey addresses a variety of WSN energy efficiency issues. However, it is predicated primarily on energy-efficient solutions that incorporate QoS Assurance for WMSNs. This research provides an analytical survey concentrating on energy-efficient routing protocols in WSNs. Our poll focuses on energy-efficient routing methods in WSNs, and it can assist readers in determining which energy-efficient routing strategy is ideal for their network. In addition, by providing an exhaustive inventory of newly proposed routing protocols, our work reflects the current state of routing research. In addition, we evaluate the advantages and disadvantages of each protocol and provide metrics (scalability, multipath,

mobility, power usage, route metric, periodic message type, resilience, and QoS support).

Secured Routing Energy Efficient Protocol (Sreep)

Each node in the network has an ID which is known in advance by the base station and cluster heads. Along with the ID, each node has a key which is preloaded. Each node in the network is aware of the location of its CH and the neighboring nodes. The (ID, KEY) pairs of the nodes are stored in a table at all the nodes of the network. We have two sink nodes which aggregate data from all the CHs in the sensing region. The secure route is constructed considering the sinks as the destination node. The packet transmitted by the nodes reach the sink even if there are malicious nodes in the transmission route. It guarantees that the message is originated from the authenticated source node and is not tampered on the route. In our secure route discovery, the malicious node on the route can be detected. Therefore, the route created using our route discovery protocol is secure.

- The routing packet and data packet are very small because they only include the partial path information.
- We create the route first, and then we forward the data to the sink node along the route.
- It only uses high efficient symmetric cryptographic operations to secure messages.

Route Discovery

The CH initiates the route discovery process through sending the route request to the sink node. When the sink node receives the request, it creates the route reply to the source CH. After the route discovery, every node along the route has established the appropriate routing table. Each CH initiates route discovery by sending the route request packet to the neighboring CHs. The route request is constructed as follows:

$$\{CH(src)ID|S(i)ID|R(req)ID|HC|MC(KCH(src),CH(src)ID|S(i)ID|R(req)ID|HC)\}$$

R(req)ID contains the (ID,KEY) of the source CH and HC is the Hop Count and it is initialized to 0 by the source CH. The intermediate CHs accept R(req)ID and increments by 1 before it transmitting it to the next intermediate CH. When the sink node receives the R(req)ID, it gets the key of the source CH from R(req)ID, which is used to verify the MC. It only accepts the first R(req)ID, with the valid MC according to the source CH and R(req)ID. Then it stores CH(i)ID, R(req)ID and HC in the routing table.

Route Reply

The sink acknowledges the route discovery by sending acknowledgement. The route acknowledgement is constructed as follows:

$$\{CH(pre)ID|CH(nxt)ID|CH(this)ID|S(i)ID|CH(src)ID|R(ack)ID|HC|MC(KS(i),S(i)ID|CH(pre)ID|CH(nxt)ID|CH(this)ID|S(i)ID|CH(src)ID|R(ack)ID|HC)\}$$

R(ack)ID contains the (ID,KEY) of the sink. CH(nxt)ID holds the ID of the next intermediate CHs in the route. CH(pre)ID holds the ID of the next intermediate CHs in the route. CH(this)ID holds the ID of the CH which was not in the source route and happens to appear in the destination route. The source node verifies the MAC after it receives the R(ack)ID and updates the routing table.

Route Maintenance

If a sensor node has no route in its routing table when it starts to send the data, it initiates the route discovery. If the source node gets the error message after it sends data or routing packet, or it is out of the specified time, it triggers a new route discovery.

Data Forwarding

The cluster head aggregates the data from the nodes in its cluster. Then it sends it to the sink nodes. We use the cluster key to provide the secure communication in the cluster. The cluster key can be established during the cluster establishment. We use the preloaded key to secure the message which is sent to the sink node. A sensor node sends the data packet to its cluster head using the cluster key. A sensor node sends the data packet to its cluster head using the cluster key, which is constructed as follows:

$$\{CH(i)ID|NCK(data)|MC[CK,CH(i)ID|NCK(data)]\}$$

Where CH(i)ID is the ID of the cluster head, and CK is the cluster key shared by the nodes within the cluster. The node with the same ID as the ID embedded in the data packet such as the cluster head verifies the MAC. If the verification succeeds, it decrypts the data using the cluster key. Then it aggregates the data from the sensor nodes in the cluster, and constructs the data packet which will be sent to the sink node. The cluster head becomes the source node after it aggregates the data. If there is a route in the routing table, it constructs the following data packet:

$$\{CH(i)ID|S(i)ID|CH(i)CK(data)|HC|MC(KCH(i),CH(i)ID|S(i)ID|CH(i)CK(data)|HC)\}$$

After the sink node gets the data packet, two operations need to be executed: 1) the sink node compares the replies from other cluster heads which are residing the neighboring clusters of the source node; 2) the sink node will compare the replies with the history record.

If the data packet is abnormal, the sink node must verify it by sending a query to the CH. This can be constructed as follows:

$$\{CH(i)ID|S(i)ID|CH(i)CK(data)|S(q)|MC(KCH(i),CH(i)ID|S(i)ID|CH(i)CK(data)|S(q))\}$$

The sink node continues the further analysis after it receives the further result from these nodes.

Security Analysis

We divide the attacks into two categories according to the compromised nodes. First, the source node is a normal node, but the intermediate node is a malicious node; the second, the source node is a malicious node. If the intermediate node is a malicious node, it can perform the following three actions: 1) Broadcast 2) Drop 3) Modify.

Intermediate Node broadcasts messages:

In the R(req)ID process, the intermediate node broadcasts the updated R(req)ID and creates the routing table. The malicious node (Node M) may have three choices to attack this process:

Case 1, it updates the R(req)ID by inserting the wrong ID of the current node;

Case 2, it does not create the routing table, or it creates it with the wrong information;

Case 3, it updates the R(req)ID by inserting the wrong ID of the previous node.

Case 1: When the R(req)ID reaches the malicious node M, it is updates the wrong ID of the current node. Other nodes drop this R(req)ID since their ID does not match the tampered ID. The node N detects that its previous hop is a malicious node since it cannot hear its rebroadcast. Then it refuses to broadcast other R(req)ID and the sink node selects other routes during next route discovery.

Case 2: When the R(req)ID packet reaches Node M, it inserts incorrect information in its routing table. Node N can detect the tampered R(req)ID broadcasted by Node M since its routing table stores two previous hops. It blacklists Node M.

Case 3: If Node M broadcasts the R(req)ID with the wrong ID of its previous node, the previous node can detect it through comparing its ID with the ID of the previous node embedded in the R(req)ID. It blacklists the malicious node M and informs the source node. The source node blocks the malicious node M.

Intermediate Node Drops Messages

In the route discovery, if a malicious node drops the R(req)ID packet, it blocks itself. The sink node can receive the R(req)ID packet through other routes. If the malicious node (Node M) drops the R(req)ID packet, the next hop (Node N) can detect it since it cannot receive the packet again. In a data forwarding process, if a malicious node drops the data packet, the sender can detect it since it cannot get acknowledgement from the next hop. It will inform it to the source node.

Intermediate Node Modifies Messages

In the route discovery, if a malicious node modifies the R(req)ID core content, such as the sink node can detect it through verifying the MAC. It drops the corrupted R(req)ID packet, and receives it from other routes. If a malicious node modifies the R(ack)ID core content, such as the source node can detect it through the MC. In the data

forwarding, we use the same solution as the case of the modified R(req)ID core content through verifying the MC.

Source Node is a Malicious Node

If the source node is a malicious node, it tries to send abnormal messages to the sink node. The sink node can detect this after it compares the data with the record in the history and the neighboring node's report. Then it sends the further request to the nodes in the cluster, and waits for the replies from these nodes for the further analysis.

V. SIMULATION RESULTS

The simulation is done through NS2 simulator. The parameters such as energy consumption, transmission time, delay and throughput are discussed in the results. The performance of the proposed algorithm is compared with few existing algorithms namely SPIN and LEACH.

Table .1. Simulation Parameters

Parameter	Value
Network size	100 m x 100 m
No. of sensor nodes	100
Radio propagation range	200 m
Channel capacity	1 M bits/s
Initial energy	1000 J
Data packets	1800 bits
Simulation time	180 s
ϵ_{fs}	100 pJ/bit/m ²
ϵ_{mp}	0.0124 pJ/bit/m ⁴

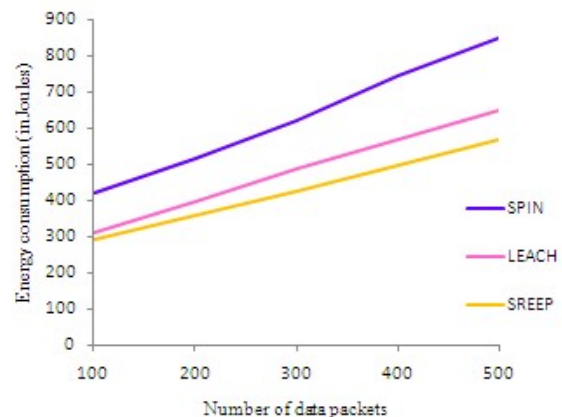


Fig. .1. Energy Consumption

The proposed algorithm SREEP consumes less energy compared to the other existing algorithms. SREEP consumes an average of 429.4 J, LEACH consumes 482.4 J and SPIN consumes 629.6 J of energy during the routing phase.

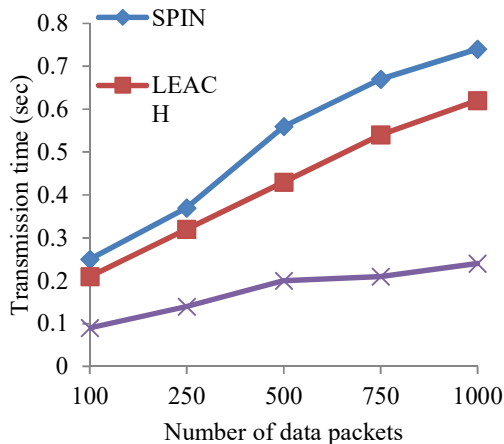


Fig. .2. Transmission Time

The proposed algorithm transmits data packets quicker than the other two existing algorithms. SREEP consumes an average time of 0.176 sec to transmit an average of 1000 data packets whereas LEACH consumes 0.424 sec and SPIN consumes 0.518 sec. The proposed algorithm has minimum delay than the other two existing algorithms. SREEP has an average delay of 0.151 sec to transmit an average of 1000 data packets whereas LEACH consumes 0.282 sec and SPIN consumes 0.267 sec.

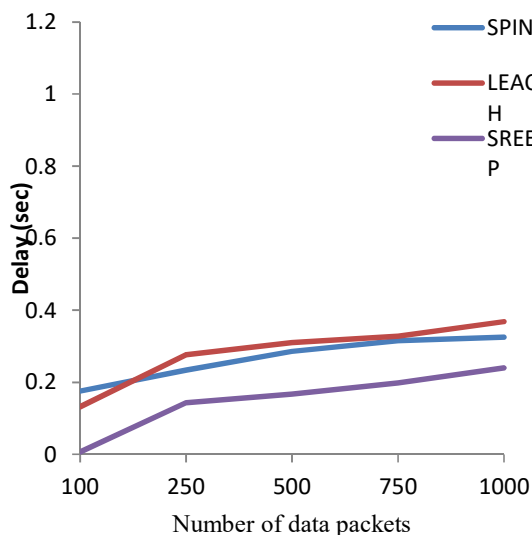


Fig. .3. Delay

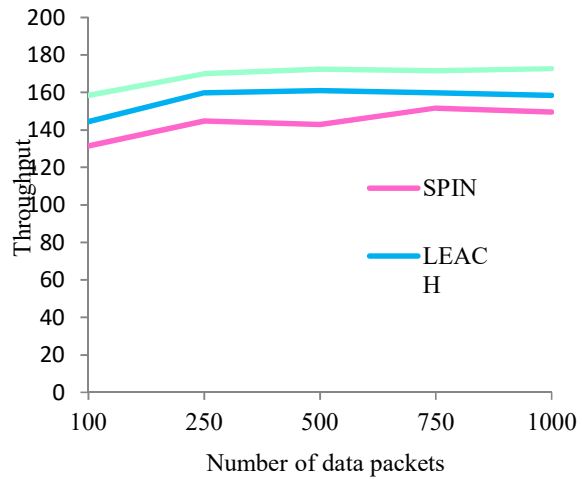


Fig. 4. Throughput

The suggested approach has a higher throughput than existing routing algorithms. SPIN has a throughput of 246 bps and LEACH has a throughput of 352 bps. When the proposed algorithm is compared to the existing one, it is discovered that the proposed approach achieves a throughput of 396 bps in 5 seconds. As a result, the suggested technique may efficiently route data packets in a given time.

VI. CONCLUSION

Compared to other current algorithms, the proposed SREEP algorithm is more energy efficient. Additionally, the method has a low transmission time and latency, guaranteeing reliable data transmission. Prior to routing, the algorithm determines the shortest path to drains. As a consequence, the cluster heads will be able to send data to the washbasin based on its proximity, thereby reducing energy consumption. In addition to providing effective security, the algorithm identifies potentially hazardous path nodes and reroutes traffic. Each time the CH wishes to transfer data, a new route is constructed, assuring the reliable transmission of data packets.

REFERENCES

- [1] Nomman Shabir, Syed Rizwan Hassan, Routing Protocols for Wireless Sensor Networks, Wireless Sensor Networks Insights and Innovations, New Zealand, 2017.
- [2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, 2002, Vol. 38, Issue 4, pp. 399-422.
- [3] Al-Karaki, A. Kamal, "Routing Techniques in Wireless Sensor networks: A Survey," Security and Networks, 2004, Vol. 11, Issue 6, pp.6-28.

- [4] S. Guo, O. Yang, "Energy-Aware Multicasting in Wireless Ad hoc Networks: A Survey and Discussion," *Computer Communications*, Elsevier, 2007, Vol. 30, Issue 9, pp. 2129-2148.
- [5] J. Yick, B. Mukherjee, D. Ghosal, "Wireless Sensor Network Survey," *Computer Networks*, 2008, Vol. 52, Issue 12, pp. 2292-2330.
- [6] G. Anastasi, M. Conti, M. Francesco, A. Passarella, "Energy Conservation in Wireless Sensor Networks: A survey," *Ad Hoc Networks*, 2009, Vol. 7, Issue 3, pp. 537-568.
- [7] R. V. Biradar, V. C. Patil, S. R. Sawant, R. R. Mudholkar, "Classification and Comparison of Routing Protocols in Wireless Sensor Networks," *Special Issue on Ubiquitous Computing Security Systems*, 2009, Vol. 4, Issue 2, pp. 704-711.
- [8] R. Yadav, S. Varma, N. Malaviya, "A Survey of MAC Protocols for Wireless Sensor Networks," *UbiCC Journal*, 2009, Vol. 4, Issue 3, pp. 827-833.
- [9] S. Ehsan, B. Hamdaoui, "A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks," *IEEE Commun. Surveys Tuts.*, 2011, Vol. 14, Issue 2, pp. 265-278.
- [10] Chen, H., Sezaki, K., Deng, P., So, H. C., "A Routing Algorithm for Mobile Multiple Sinks in Large-Scale Wireless Sensor Networks," In *Proceeding of the 3rd IEEE Conference on Industrial Electronics and Applications*, 20-23 August 2008, pp. 1557-1561.
- [11] Dr. Nagarajan Munnusamy, Sneha Vijayan, Ezhilarasi, M. "Role of Clustering, Routing Protocols, MAC protocols and Load Balancing in Wireless Sensor Networks: An Energy-Efficiency Perspective", *Cybernetics and Information Technologies (Open Access)*, ISSN 1314-4081, Volume 21, Issue 2, June 2021.
- [12] M. Ezhilarasi, V. Krishnaveni, "A survey on Wireless Sensor Network: Energy and Lifetime Perspective", 2018, *Taga Journal*, vol 14, pp. 3099-3113, ISSN: 1748-0345.
- [13] M. Nagarajan, S. Karthikeyan, "A New Approach to Increase the Lifetime and Efficiency of Wireless Sensor Network", 2012, *IEEE International Conference of Pattern Recognition, Informatics and Medical Engineering (PRIME)*, pp. 231-235.