Correlation Distance Based Greedy Perimeter Stateless Routing Algorithm for Wireless Sensor Networks

S.Venkatasubramanian
Department of Computer Science, Saranathan college of Engineering, Trichy-12
Email: veeyes@saranathan.ac.in

ABSTRACT

Wireless sensor networks (WSNs) are a popular study topic because of the extensive range of potential applications they have. A WSN is made up of a few hundred to tens of thousands of sensor nodes from anywhere, all of which interconnect via radio signals. Restrictions on computing power, storage, battery life, and transmission bandwidth are all factors to consider while designing a WSN. Clustering and routing procedures have been proposed to deal with these problems. Wi-Fi sensor network routing is a critical but tough task. A Greedy Perimeter Stateless Routing (GPSR) algorithm, an effectual and receptive routing system is developed. Packet forwarding decisions are based on node placements. When transferring messages, the GPSR always takes the shortest route possible between the source and destination nodes. Using distance measurements including Euclidean, city block, cosine, and correlation, the complete weighted directed graph is constructed in this study. Rigorous simulation has been executed using NS-2. Also, the GPSR performance with different distance measures is compared and validated. The results show that the proposed GPSR with correlation distance provides better performance in terms of packet delivery ratio, throughput, routing overhead and average stability time of cluster head, when compared to other distance measures.

Keywords - **Complete Weighted Directed Graph, Clustering, Greedy Perimeter Stateless Routing, Packet Delivery Ratio, Wireless Sensor Network.**

Date of Submission: Nov 10, 2021 Date of Acceptance: Dec 10, 2021

I. INTRODUCTION

There are multiple sensors in a WSN that collect data from the surrounding environment and send it to a central station (BS) [1]. The main impartial is to keep track of things, collect info, and send it to the base station. The data acquired by sensor nodes located across the field can be used to produce the most accurate report possible about the surrounding areas. Measurement of physical parameters, such as pressure, moisture, and temperature is carried out by several WSNs organized in a network to improve the fidelity of stated metrics while also collecting information that reduces communiqué overhead in the network, ultimately leading to significant energy savings. WSN becomes increasingly attentive as a result of features such as low power consumption, low cost, and sensor nodes that can perform several functions [2-4].

WSN has recently been used in numerous real-world applications, including home security, military surveillance, non-domestic animal behavior monitoring, and healthcare services, thanks to advancements in cloud technology. Widespread research is now being done to explore WSN in previously unexplored long and large areas [5]. When building a sensor network, it's important to keep in mind that all of the components are physically constrained. In unmanned environments, WSN damages the nodes, necessitating the purchase of new or more costly nodes [6]. A longer compute time without power is required in many circumstances, hence the wireless node must be used. As a result, while designing a network router under the situation of a long network lifespan, energy efficiency becomes a major concern. Familiarizing the network topology and altering the router's energy-level sensors could improve and maintain energy conservation [7-8].

The clustering approach is used in routing protocols to reduce power consumption [9]. To perform sensing operations, the sensor nodes with the lowest power consumption are obtained, and the data collected during sensing is transmitted to the cluster head (CH) across a short distance. Using a CH node, data from the other members of the cluster can't be correlated, which reduces the overall amount of data transferred to the back-end system [10]. The architecture for clustering is shown in Figure 1.

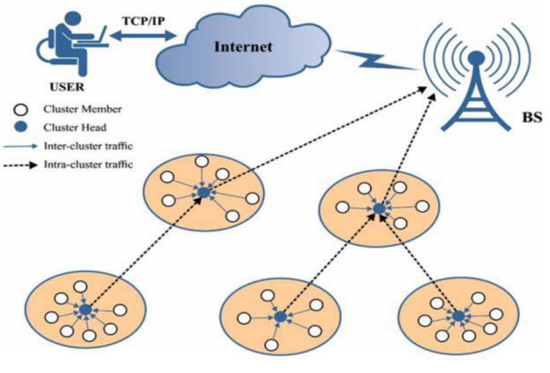

Figure 1. Process of Clustering in WSN

It is possible to increase energy efficiency by clustering by minimizing overall power preservation and handling it among nodes while taking network lifetime into consideration [11]. Furthermore, it is capable of reducing channel content and data collisions, resulting in increased network throughput under high load. Several routing strategies are designed to extend the life of a network based on constraints like limited energy, bandwidth, and processing power.

The sensor node's battery power is depleted proportionately to the amount of data it broadcasts during WSN operation [12]. This demonstrates that a significant portion of the node's energy is consumed during communication. In order to extend the lifespan of WSNs, good data routing is required between the routing algorithms and the communication activities among the sensor nodes. The majority of the early work on WSN routing protocol took sensor nodes with uniform data rates into account. A WSN sensor node's energy and data rate may vary widely in real-world applications [13]. They could cause unequal energy consumption and an imbalanced load across the network if not appropriately utilized, which would harm network performance.

The existing techniques also use the greedy routing protocol for finding the shortest distance, however, they use only Euclidean distance to form the complete weighted graph. In addition, this single distance measure increases the energy consumption of the network for whole data transmission. But, the research work proposed the GPSR with four different distance measures to find the shortest path for routing in WSN to improve efficiency and consume less energy. The experiments are carried out using NS-2 simulator and validated with different metrics. The remaining paper is classified as: Section II comprises the related work with geographical routing. Section III provides a detailed explanation of GPSR with four distance measures. The validation of the proposed method with different metrics is given in Section IV. Finally, the scientific contribution of work with future work is provided in Section V.

II. RELATED WORK

A reservation-based CH assortment is proposed in [14] to minimize clustering's overhead energy consumption. This method eliminates the requirement for network nodes to transmit messages contending for a time as a CH by allocating CH time to each node. CHs are chosen using a LEACH-based technique in the first round. Each node in the reservation phase chooses which round it will be the CH and creates an arrangement matrix with one row and R columns. Nodes then assign entries with 1 to rounds in which they will act as CH, and with 0 to rounds in which they will act as normal nodes. Each node communicates its reservation matrix to all other nodes after the reservation phase has ended. This matrix is used to create a larger matrix known as the total matrix. This matrix is exposed to all other nodes and shows which node will be CH in each round R. A key CH selection criterion is omitted, thus even if this strategy reduces message overhead, it's still assumed to be inefficient. These contain residual energy, node density, and so on, and are only appropriate for small networks because storing the whole matrix in each node takes up a large amount of memory space. Furthermore, there is no thought given to reducing the amount of redundant data sensing and transmission inside the network. Despite the fact that the preceding measures have improved network performance, they have not eliminated redundant data communication from sensor nodes that are located near together in densely deployed WSNs.

It was found that traffic and energy heterogeneity had a negative impact on the SEP algorithm's performance [15]. Nodes with regular traffic and progressive nodes with heavy traffic are used to simulate two-level energy heterogeneity in this study instead of the original SEP's two levels of energy heterogeneity. As traffic volume increases, SEP's performance drops dramatically, according to the findings. Sharma et al. [15] suggested a new strategy for selecting CHs that performs better in heterogeneous environments. High traffic nodes will continue to generate more data even if an adequate CH is selected, and this could lead to early depletion of the energy in that node. Due to its design for two-level communication, this protocol is not appropriate for WSN with several levels of heterogeneous sensor nodes.

An energy and traffic heterogeneous sensor network known as TEAR protocol was created to deal with this problem in [16]. Because of this, many levels of energy and data creation rate discrepancies (multi-level heterogeneity) are taken into account in TEAR. In TEAR, the probability of a CH election is based on the beginning and residual node energy, traffic load, and the round's average energy. Using the TEAR protocol, nodes with high traffic and low energy are not chosen for the CH function, but those with high energy and low traffic rate are. Due to the high data rate, the low-energy node with high traffic will perish faster than the top-energy node with low traffic. Modelling a realistic WSN is facilitated by using the TEAR technique. However, it lacks essential energy-saving mechanisms, such as reducing redundant data transmission and conserving and decreasing the fast energy consumption of high-traffic nodes.

Another traffic heterogeneous network routing system termed Distributed Efficient Fuzzy Logic (DEFL) based routing is projected in [17] to reduce the energy consumption of high traffic nodes. This protocol treated nodes as heterogeneous entities with differing amounts of traffic. For this algorithm, the shortest path had the lowest cost. The major goal of this strategy is to steer clear of routes with heavy traffic. Traffic rate, energy, and node residual energy are all fed into the fuzzy in DEFL. Using this method extends the network's life by removing the message relaying strain from nodes with high traffic. As a result of this design flaw, nodes in close proximity to the observed event will continue to experience performance issues due to the high volume of traffic. In addition, this strategy made use of flat routing, which exacerbates the network's communication problems and reduces overall network performance.

2.1.1. Geographic Routing

Greasy mode, or greedy advancing, is a technique that uses nodes in its one-hop range to determine which nodes are nearest to the destination. Our work is based on prior studies [18-19] that assumed a radio range form as an ideal circle surface and investigated each method for face routing. For each of these nodes, it determines which node in the intersection area of the circle and its radio range is the most likely candidate for serving as a gateway between it and the destination node. Due to the fact that greedy forwarding employs local info in the one-hop range, the network topology does not have to be used entirely. However, due to the following restriction, greedy forwarding does not always send data packets to the destination node [20-21]. If you look at Figure 2, there aren't any suitable nodes near where the source node s is, hence it fails to send the data packet. As a result of WSN's characteristic of placing sensor nodes at random, situations like the one shown in Figure 2 are common. Perimeter mode, which is recovery mode, is used by geographic routing to deal with the breakdown of data packet transmission.

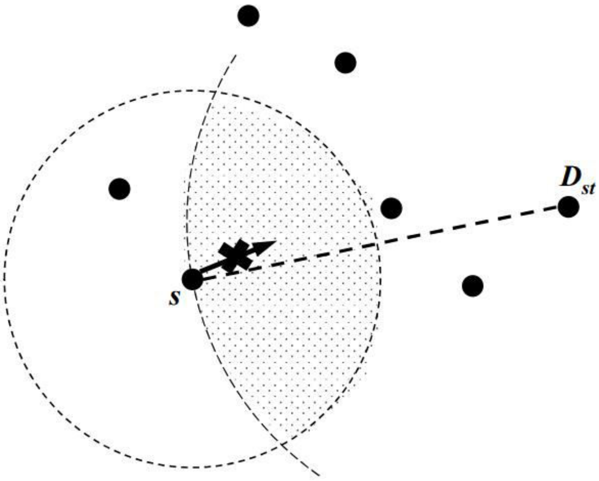

Figure 2. Data transmission at Greedy forwarding failure during

When delivering data packets, each source node sends two burst packets, one on the right and the other on the left side of the hole, in order to better balance the load. This technique was developed by Huang et al. [22]. Due to the high overhead of transmitting burst packets across nodes, these approaches may lead to increased sensor node energy consumption.

III. PROPOSED ALGORITHM

GPSR is a WSN routing protocol that is fast and responsive [23]. GPSR, in contrast to other routing protocols, takes into account the relationship between a sensor network's physical location and its communication. When deciding how to forward packets, the nodes' placements are taken into consideration. Packets are forwarded to nodes that are gradually becoming closer to the destination node using greedy forwarding.

When there is only one path to the target node in the sensor network because of the lack of greedy paths, one path must be temporarily moved away from the node. It can be recovered by advancing in perimeter mode, which sends a packet to each node in turn along a planar sub-graph of the whole radio network joining graph. The greedy forwarding continues when it gets to a node that is nearer to the destination node than the current node. A self-maintaining routing strategy for wireless sensor networks, Dynamic Source Routing (DSR), is yet another routing protocol to consider. DSR [24] is capable of configuring and organizing the network on its own, without the need for human intervention. Depending on the source, the DSR will utilize a different route to send the data packets. This process comprises two phases: Route Discovery and Route Maintenance. Route discovery identifies the best route for transmitting data between the source and destination nodes.

To ensure that communication routes are always optimal and loop-free even if network conditions change, route maintenance ensures that communications routes are changed as they are being transmitted. Our model's security protocol protects against assaults from the inside as well as the outside, including active and passive attacks [25].Inside the network, an attack can be stopped and the attacker can be avoided. However, precautions should be implemented in the network to protect against an assault from the outside. When a data packet is being actively attacked, not only are the contents tampered with but so is the routing information that is passed along with it. By contrast, data packets are unaffected by passive attacks while they are being transmitted. In a mote class attack, the attacker's capabilities can be compared to those of a sensor node. Laptop-based attacks, on the other hand, are more computationally and strategically sophisticated. Data transfer is safe and secure when using several paths. When calculating energy, it uses the average data from sensor nodes. Security and energy efficiency are two important criteria to look for in a system like this. As opposed to sensor nodes, base stations have the ability to calculate power and compare energy. As soon as the BS has decided on a path, communication can begin. Figure 3 shows the workflow of the proposed methodology.

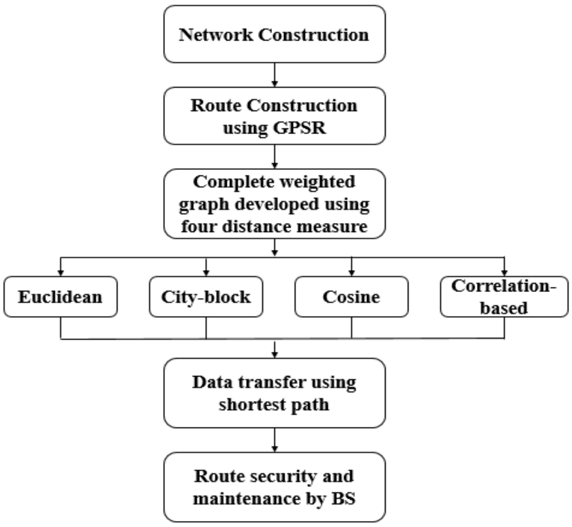
Network Construction
Route Construction using GPSR
Complete weighted graph developed using four distance measure
Euclidean
City-block
Cosine
Correlation-based
Data transfer using shortest path
Route security and maintenance by BS

Figure 3: Working Flow of the proposed methodology

3.1. Network

In mobile Ad-hoc networks, nodes can be dynamically moved across the network, whereas in WSN, nodes are permanently put in one location. On the other hand, a static network has been implemented in a WSN. The secure multipath routing will only be appropriate for networks that use solely static wireless sensors. As a result, we're putting together a network of wired sensor nodes from scratch. The sensor nodes themselves are varied. The node's initial energy level is fixed. After distribution, sensor nodes can't be re-energized; if their energy runs out, they're deemed "dead nodes."

The primary goal of the network is to create clusters and then choose the cluster leaders from among those clusters. Sensor nodes are randomly distributed in this network and remain static after distribution. Sensor nodes take data from the field, process it, and send it to the base station based on their sensing capabilities. One unique shared key is shared between the sensor nodes and BS. Each sensor node has its own unique ID.

3.2. Route Construction

Multipath routing divides a message into packets, each of which travels along a distinct path. Multipath routing alters the transmission order of packets. Data transmission reliability can be improved by using secure multipath routing. To keep packet order, we'll need to include some metrics, such as a sequence identifier. Routing requests RREQ packets will be sent from the base station to each sensor node. It will then broadcast to its neighbors in order to accumulate. As soon as nodes get a route request message, the list of their nearby nodes is updated. As the RREQ is being accumulated, packet broadcast is being received throughout the network. Use the base station's public key to authenticate a neighboring node. Authentication will fail if the key does not match, and the node will not add any new neighbors. It will update the previous node with the address of the current node after receiving the previous node's address. When a route request and packet sequence number are included in a received message list, it won't be resent. Instead, the Sequence Number of the packet will be retained in the Received message list, and it will be resent now. The RREQ packet is delivered to every sensor node to obtain a list of their neighbors. A node's neighbor list can be used to get information about how nodes connect.

The node will receive a Route Request message from the BS at a specific time. As a result, the base station is forced to wait. After waiting for the node to submit the Route Collection message, the BS will send it to the entire network, which is also known as RCOL. The sensor node's network will be connected to the node next to it to disseminate the message. When a node receives a route collection message from the base station after receiving a Route Request broadcast, the process described above is repeated. After that, each node in the network broadcasts the entire network's state.

The response packet is routed to the base station when the sensor node gets RCOL. This holds information about the current node, address, and the amount of energy used during data transmission between nodes. As well as the neighbor list and energy used during transmission, the base station has a list of all nodes. The weighted directed graph can be constructed using this information base station. $G = (N, E)$gives us the complete weighted directed graph. $N$is a collection of nodes, whereas E denotes a collection of routes connecting all of the sensors. There are two variables i and jth at describe the placements of the nodes. Sensor nodes i and j are separated by an E-distance, therefore the energy between them is given by E_{ij} and constructed the whole weighted graph. The E_{ij} is defined by four different spaces in this suggested work. These distances are specified as follows: Euclidean distance, city block distance, cosine distance, and correlation distance.

The Euclidean distance between two points $i = (x_1, x_2, x_3, .. x_n)$ and $j = (y_1, y_2, y_3, .. y_n)$ is computed using the eqn. (1)

$$\text{Euclidean distance}_{i,j} = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2} \qquad (1)$$

The city block distance between two points $i = (x_1, x_2, x_3, .. x_n)$ and $j = (y_1, y_2, y_3, .. y_n)$ is computed using the eqn. (2)

$$\text{city block}_{i,j} = \sum_{i=1}^{n} |x_i - y_i| \qquad (2)$$

The cosine distance between two points $i = (x_1, x_2, x_3, .. x_n)$ and $j = (y_1, y_2, y_3, .. y_n)$ is computed using the eqn. (3)

$$\text{cosine}_{i,j} = \frac{\sum_i x_i y_i}{\sqrt{\sum_i {x_i}^2}\sqrt{\sum_i {y_i}^2}} \qquad (3)$$

The correlation distance between two points $i = (x_1, x_2, x_3, .. x_n)$ and $j = (y_1, y_2, y_3, .. y_n)$ is computed using the eqn. (4)

$$\text{correlation}_{i,j} = \frac{N\sum xy-(\sum x)(\sum y)}{\sqrt{[N\sum x^2-(\sum x)^2][N\sum y^2-(\sum y)^2]}} \qquad (4)$$

To send a packet of data, the base station determines the shortest way from that four distance calculation metric and then uses that path to transfer the data packet. The base station also gathers data on things like energy and distance between nodes.

3.3. Data Transfer

The power consumption of a sensor node varies depending on its location. The data is sent over the shortest and most efficient path, which is determined during the route development process. The network knows how much energy it takes to transmit each item of data. The base station sends DREQ data requests to all network nodes. Data request packets arrive at the sensor node and are responded to by data reply DEP packets (data response data). When a node receives a data request from the base station, it goes through a series of steps before returning any data. With the help of a special shared key, Node authorizes the communication. If the shared key matches, it accepts the packet. For the duration of its life, the node connects to the base station using the same unique shared key. The node will not convey data if the destination node is the same as the present node, because the source and destination nodes are the same.

Messages that are not intended for the Current Node are replayed to the neighbor list. The ideal path is chosen after data has been collected from all nodes rendering to a previous phase by the BS. The base station selects the best path and then sends a routing request. It is expected that a route acknowledgment packet will be sent from the sensor node in response to this message. Instead of a data reply, an error packet ERRP is transmitted when the security key does not match.

Authorizing the key takes less time and effort. When a sensor node detects something, it transmits data packets to the central station. The sensor node transmits the data packets to the central station. When a BS must wait a particular amount of time before receiving a data reply, it will consider that route to be under attack by the attacker if it does not receive one by that time. To choose the best route, data request messages are delivered via several optimal routes to the network.

3.4. Route security and Maintenance

If a sensor node fails to approve the key or has insufficient energy, it will be withdrawn from the network or the path, and the network will take alternate paths. The sensor nodes also send an error reply packet as an information update. The base station determines the route, not the source or destination. If an error message is sent due to a failure in authorizing the public key authentication or because of a hostile node in the sensor network, the BS switches the data transfer route. This can be because of the physical environment or an attack by assailants. The performance of the proposed GPSR will be validated in the next section.

VI. RESULTS AND DISCUSSION

A wireless network environment, including nodes, clusters, and bases, was developed for the proposed technique using the NS2 simulator in this research. Here, we've set up a network with 53 nodes, with Node 6 as the source node and node 44 as the destination node. Nodes 13 through 49 are used in the routing process. The encryption and decryption of data are made secure by using a shared public key. Table.1 shows the network and sensor node parameters assigned to each of the nodes.

TABLE 1. Simulation Parameters

Parameter	Value
simulation time	80s
the initial energy of node	200J
wireless communication line bandwidth	1Mbps
time of each round	20s
size of the packet header	25Bytes
network monitor area	1500m×1050m
Deployed number of sensor nodes	53
data size of packet	500Bytes

4.1 Performance parameters

This subsection details the parameters that measure the working of four different distance calculations such as Euclidean Distance (ED), City Block Distance (CBD), Cosine Distance (CD), and Correlation Distance (CoD). Experimental is carried to find packet delivery ratio, throughput, routing or overhead, and stability period of cluster head to draw the comparison of four different distance calculations.

4.1.1. Packet delivery ratio (PDR)

PDR is the proportion of packets that destinations receive to those that sources originate. PDR can be described mathematically as follows: S1/S2 where S1 is the total number of data packets received by each endpoint and S2 is the total number of data packets produced by each source as specified in the equations (5)

$$PDR(\%) = \frac{Number\ of\ packets\ received}{number\ of\ packets\ sent} * 100 \qquad (5)$$

4.1.2. Throughput

The equation states that it is the ratio of the total amount of packets sent to the whole simulation duration

$$Throughput(kbps) = \frac{recrived\ packets\ (bytes)*8}{1024*(stop\ time-start\ time)} \qquad (6)$$

4.1.3. Routing Overhead

Network overhead is the number of control (hello packets) and routing packets required for an overall network communication illustrated in equation (7).

$$Overhead\ (in\ ratio) = \frac{Total\ control\ and\ routing\ packet}{number\ of\ data\ packets\ received} \quad (7)$$

4.1.4. Stability time period of cluster head

The stability of a cluster head node is defined as the time period for which the node worked as a cluster head of the cluster. The average of that time period is known as average stability time.

4.2 Experimentation and result analysis

In this section, the performance of GPSR in terms of four different distances are tested and compared in terms of PDR, which is given in Table 2, and graphical representation for this experiment is provided in Figure 4.

Table 2. Validated Analysis of Proposed Method for Packet delivery ratio.

Number of nodes	ED	CBD	CD	CoD
20	75.68	82.5	84.32	89.11
40	74.74	84.6	86.43	93.76
60	69.02	85	88.01	95.1
80	69.87	85.8	89.15	96
100	77.97	88	92.21	97.43

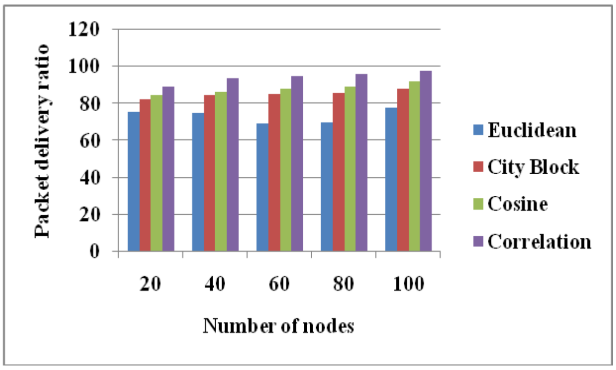

Figure 4: Graphical Representation of Proposed Method in terms of PDR.

When the number of nodes is 20, the ED has only 75.68% of PDR, CBD has 82.50% of PDR, CD has 84.32% of PDR and CoD has a high PDR value (i.e. 89.11%). When comparing with all distances, ED has low PDR values for every node, for instance, ED has nearly 69% to 77% of PDR when the nodes are 40, 60, 80, and 100. As with ED, CBD has nearly 84% to 88% of PDR, when the nodes are 40, 60, 80, and 100. The CoD has 93.76% of PDR and CD has 86.43%, when the node is 40, where the CoD achieved nearly 97% of PDR and CD has only 92.21% of PDR, when the node reaches 100. This proves that when the nodes are increased, the performance of CoD is also increased in terms of PDR. Te next Table 3 shows the performance of these four distances in terms of throughput and Figure 5 shows the graphical representation for the same.

Table 3: Validated Analysis of Proposed Method for Throughput (kbps).

Number of nodes	ED	CBD	CD	CoD
20	98	110	126	136
40	110	124	157	166
60	138	135	176	189
80	149	180	220	234
100	172	210	255	263

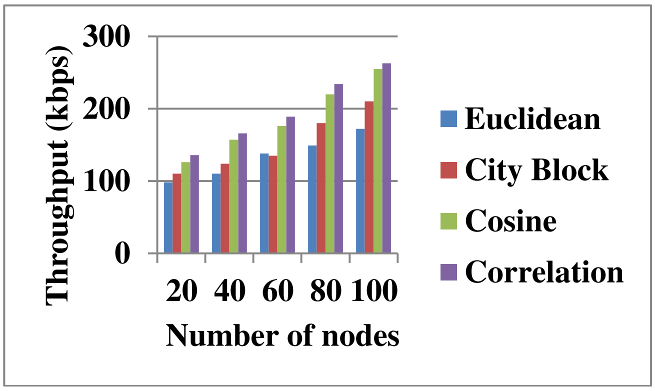

Figure 5: Graphical Representation of Proposed Method in terms of throughput.

The throughput of the proposed GPSR for each distance is increased, when the number of nodes is also increased. In the throughput experiments, the ED has 98kbps, CBD has 110kbps, CD has 126kbps and CoD has 136kbps, when the node reaches 20. These same techniques achieved 138kbps, 135kbps, 176kbps, and 189kbps, when the node reaches 60. Finally, when the node reaches the final, the ED has only 172kbps, CBD has 210kbps, CD has 255kbps and CoD has 263kbps throughput. This experiment proves that the GPSR-CoD achieved better performance than other distance measures of GPSR. Table 4 and Figure 6 show the experimental analysis of the proposed method for routing overhead.

Table 4. Performance Analysis of Proposed method for Routing Overhead

Number of nodes	ED	CBD	CD	CoD
20	0.6	0.4	0.4	0.4
40	0.8	0.6	0.5	0.4
60	0.9	0.7	0.62	0.53
80	0.98	0.9	0.82	0.75
100	1.23	1	0.96	0.83

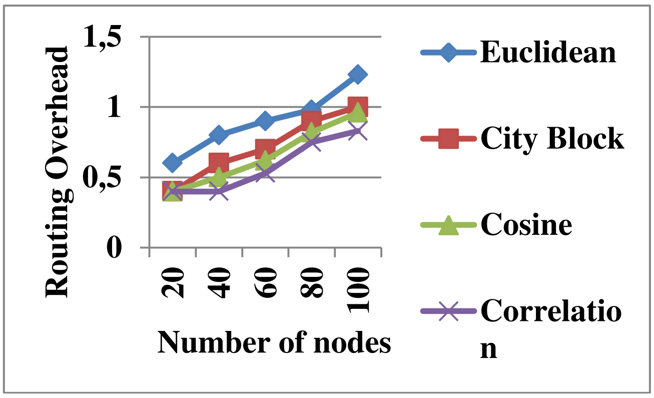

Figure 6: Graphical Representation of Proposed Method in terms of Routing Overhead.

The routing overhead of CBD, CD, and CoD is stable (i.e.0.4), the ED has 0.6 of routing overhead, when the node is 20. The ED has 0.8, CBD has 0.6, CD has 0.5 and CoD has 0.4 of routing overhead, when the node reaches 40. These same techniques achieved 0.98, 0.9, 0.82, and 0.75 of routing overhead when the node reaches 80. These experimental results show that several nodes influence the performance of routing overhead of each distance measure of GPSR. Table 5 and Figure 7 shows the validation analysis of various distance measure of GPSR in terms of the average stability time of CH's.

Table 5. Validation Analysis of Proposed Method in terms of Average Stability time of CH's (sec)

Number of nodes	ED	CBD	CD	CoD
20	10	15	22	22
40	30	40	50	55
60	40	60	75	80
80	55	75	88	94
100	65	95	110	120

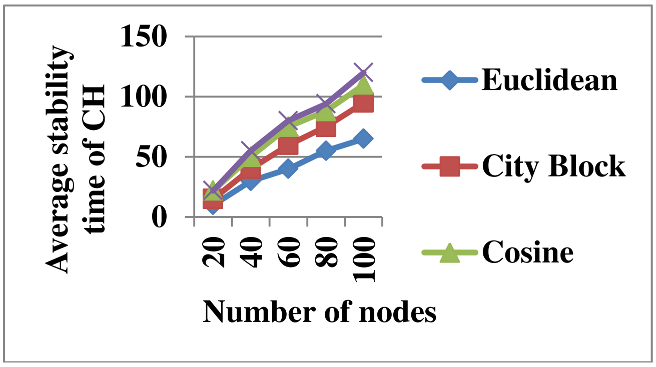

Figure 7:Graphical Representation of Proposed Method in terms of Average stability time of CH.

When the node is less, the stability time of each distance measure is also less. For instance, the ED has 30sec, CBD has 40sec, CD has 50sec and CoD has 55sec, when the node is 40. As like, the ED has 40sec, CBD has 60sec, CD has 75sec and CoD has 80sec, when the node is 60. In the other set of experiments, the ED has 55sec, CBD has 75sec, CD has 88sec and CoD has 94sec, when the node is 80. Finally, the ED has 65sec, CBD has 95sec, CD has 110sec and CoD has 120sec, when the node is 100. From these above all experiments, it is proven that the GPSR-CoD achieved better performance in terms of PDR, routing overhead, throughput, and average stability time of CH's. This is because, unlike Pearson's correlation coefficient, the CoD applies to random variables of any dimension. It has also been used to detect nonlinear relationships that were previously undetected by Pearson. While ED does have some advantages, one disadvantage is that if two data vectors do not share any attribute values, their distance may be smaller than that of another pair of data vectors that does.The primary disadvantage of CBD is that they are not compatible with many standard multivariate analyses such as discriminant analysis. The reason for the poor performance of CD is that it is that the magnitude of vectors is not taken into account.

V. CONCLUSION

The WSN has applications in nearly every area of networking, and a variety of technologies are already being utilized to extend the life of the low-power network. End-to-end delay, packet loss during transmission, and lower sensor node lifetime owing to energy loss are the key drawbacks. A wireless sensor network has been developed in this research to overcome these issues. The nodes were communicated, and a list of all nearby nodes was compiled to help with path selection using GPSR. GPSR takes into account the relationship between a sensor network's physical location and its communication, unlike other routing methods. Four different distance measures such as ED, CBD, CD, and CoD are used for the completed weighted graph. The experiments are carried out to test the efficiency of each distance measure in terms of PDR, routing overhead, throughput, and average stability time of CHs. The simulation results proved that the GPSR-CoD achieved better performance (i.e.120sec of average stability time of CHs, 0.83 routing head, 263kbps of throughput, and 97.43 of PDR for the node 100) than other distance measures. The future direction of the proposed work includes the implementation of cluster-based routing protocol, applying the proposed model to refine the delay-constrained applications. Furthermore, the work can be extended by applying an evolutionary algorithm to optimize the QoS parameters of routing.

REFERENCES

[1] Chandel, A., Chouhan, V.S. and Vyas, D.. A Survey on Architecture and Protocols for Wireless Sensor Networks. In *Advances in Information Communication Technology and Computing,* 2021 127-141. Springer, Singapore.

[2] Shankar K and Elhoseny M, Trust-based cluster head election of secure message transmission in MANET using a multi-secure protocol with TDES, *Journal of Univeresal Computer Science, 25.* 1221-1239. 10.3217/jucs-025-10-1221.

[3] Dutta AK, Elhoseny M, Dahiya V, et al. An efficient hierarchical clustering protocol for multihop Internet of vehicles communication, *Transactions on Emerging Telecommunications Technologies*. 31. 10.1002/ett.3690.

[4] Elhoseny M and Shankar K., Reliable data transmission model for mobile Ad Hoc network using signcryption technique, *IEEE Transactions on Reliability. 69,* 2020 1077-1086. 10.1109/TR.2019.2915800.

[5] Uma Maheswari P, Manickam P, Sathesh Kumar K, et al. Bat optimization algorithm with fuzzy based PITsharing (BF-PIT) algorithm for Named Data Networking (NDN*). Journal of Intelligent & Fuzzy Systems. 37.* 2019,1-8. 10.3233/JIFS-179086.

[6] Arjunan S, Pothula S and Ponnurangam D. F5N-basedunequal clustering protocol (F5NUCP) for wirelesssensor networks. Int J CommunSyst2018; 31(17):e3811.

[7] Gupta, D., Khanna, A., SK, L., Shankar, K., Furtado, V. and Rodrigues, J.J., 2019. Efficient artificial fish swarm based clustering approach on mobility aware energy-efficient for MANET. Transactions on Emerging Telecommunications Technologies, 30(9), p.e3524.

[8] Elhoseny M and Shankar K. Energy efficient optimal routing for communication in VANETs via clustering model., *Emerging technologies for connected internet of vehicles and intelligent transportation system networks* (Studies in systems, decision and control, vol. 242). Cham: Springer,2019, pp.1214.

[9] Shahraki, A., Taherkordi, A., Haugen, Ø. and Eliassen, F., Clustering objectives in wireless sensor networks: A survey and research direction analysis. *Computer Networks*, *180*, 2020 p.107376.

[10] Arjunan S and Pothula S. A survey on unequal clustering protocols in wireless sensor networks. *Journal of King Saud University - Computer and Information Sciences. 31.* 2019, 10.1016/j.jksuci.2017.03.006..

[11] Arjunan S and Sujatha P., Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. *Applied Intelligence. 48.* 2018, 1-18. 10.1007/s10489-017-1077-y. 2018; 48(8): 2229–2246.

[12] Fanian, F. and Rafsanjani, M.K.,. Cluster-based routing protocols in wireless sensor networks: A survey based on methodology, *Journal of Network and Computer Applications, 142,* 2019, pp.111-142.

[13] Diwakaran, S., Perumal, B. and Devi, K.V., An intelligent data aware and energy censoring scheme for wireless sensor networks. *Cluster Computing, 22(2),* 2019, pp.4213-4220.

[14] A. Zahedi, M. Arghavani, F. Parandin, and A. Arghavani, Energy efficient reservation-based cluster head selection in WSNs,, *Wireless Personal. Communication, vol. 100, no. 3,* 2018,. 667–679,

[15] D. Sharma, A. Goap, A. Shukla, and A. P. Bhondekar, Traffic heterogeneity analysis in an energy heterogeneous WSN routing algorithm, in *Proceedings. 2nd International Conference on. Communication Computer. Networks*., 2019, 335–343.

[16] D. Sharma and A. P. Bhondekar, ‘‘Traffic and energy aware routing for heterogeneous wireless sensor networks,’’ *IEEE Communication Letters*, *vol.* 22, no. 8, Aug. 2018, , pp. 1608–1611,.

[17] R. M. Al-Kiyumi, C. H. Foh, S. Vural, P. Chatzimisios, and R. Tafazolli, Fuzzy logic-based routing algorithm for lifetime enhancement in heterogeneous wireless sensor networks, *IEEE Transactions on. Green Communication. Networks., vol. 2*, no. 2, Jun. 2018,. 517–532,

[18] Cho, E.S.; Yim, Y.; Kim, S.H. Transfer-Efficient Face Routing Using the Planar Graphs of Neighbors in High Density WSNs.Sensors2017, 17, 2402.

[19] Cho, H.; Kim, S.; Kim, C.; Oh, S.; Kim, S.H. Energy-efficient look ahead face routing using coverage range in wireless networks. *In Proceedings of the 2017 14th IEEE Annual Consumer*

Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; . 767–771.

[20] Masoud, M.Z., Jaradat, Y., Jannoud, I. and Al Sibahee, M.A,. A hybrid clustering routing protocol based on machine learning and graph theory for energy conservation and hole detection in wireless sensor network. *International Journal of Distributed Sensor Networks, 15(6).,* 2019 .1550147719858231.

[21] Parvin, S.; Sarram, M.A.; Mirjalily, G.; Adibnia, F, A survey on void handling techniques for geographic routing in VANET network. *International. Journal of Grid Distributed. Computing.*, 8, 2015,101–114.

[22] Huang, H., Yin, H., Min, G., Zhang, J., Wu, Y., & Zhang, X.,Energy-aware dual-path geographic routing to bypass routing holes in wireless sensor networks,. *IEEE Transactions on Mobile Computing, 17(6*), 2018,1339–1352.

[23] Greedy Perimeter Stateless Routing, Available: *https://www.icir.org/bkarp/gpsr/.*

[24] Routing Dynamic Source Routing , by Margaret Rouse
Available:*https://searchnetworking.techtarget.com/Dynamic-Source-Routing*

[25] Hamid, A. and Hong, C.S,. Defence against lap-top class attacker in wireless sensor network, *8th International Conference Advanced Communication Technology Vol. 1,* 2006, February . 5-pp. *IEEE.*

Author's Biography

S.Venkatasubramanian received the B.E. degree in Electronics and Communication from Bharathidasan University and M.E. degree in Computer science from Regional Engineering College,Trichy. He has 23 years of teaching experience. He is currently pursuing doctoral research in mobile Ad hoc networks. His areas of interest include mobile networks, Network Security and software Engineering. He has published 25 papers in the international journals, 10 papers in international conferences and filed 4 patents. At present he is working as an Associate Professor in Department of CSE at Saranathan college of Engineering, Trichy, India.