




## Research Article

# End-to-End Latency Analysis for Data Transmission via Optimum Path Allocation in Industrial Sensor Networks

Rajaram Jatothu <sup>1</sup>, Jaya Dipti Lal,<sup>2</sup> N. P. G. Bhavani,<sup>3</sup> K. A. Sharada,<sup>4</sup> E. Balraj,<sup>5</sup>  
Karthik Kumar Vaigandla,<sup>6</sup> Arvind Kumar Shukla,<sup>7</sup> Mohammad Ishrat <sup>8</sup>  
and Kibebe Sahile <sup>9</sup>

<sup>1</sup>Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, Telangana, India

<sup>2</sup>Department of Electronics and Telecommunication, Shri Govind Ram Sekseria Institute of Science and Technology, Indore, Madhya Pradesh, India

<sup>3</sup>Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India

<sup>4</sup>Department of CSE, HKBK College of Engineering, Bengaluru, Karnataka, India

<sup>5</sup>Department of Information Technology, M. Kumarasamy College of Engineering, Karur, Tamilnadu, India

<sup>6</sup>Department of Electronics and Communication Engineering, Balaji Institute of Technology and Science, Warangal, Telangana, India

<sup>7</sup>Department of Computer Applications, IFTM University, Moradabad, India

<sup>8</sup>Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India

<sup>9</sup>Department Of Chemical Engineering, College Of Biological And Chemical Engineering Addis Ababa Science And Technology University, Ethiopia

Correspondence should be addressed to Rajaram Jatothu; [drjrajaram81@gmail.com](mailto:drjrajaram81@gmail.com) and Kibebe Sahile; [kibebe.sahile@aastu.edu.et](mailto:kibebe.sahile@aastu.edu.et)

Received 29 April 2022; Revised 19 June 2022; Accepted 22 June 2022; Published 31 July 2022

Academic Editor: Kalidoss Rajakani

Copyright © 2022 Rajaram Jatothu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In a sensor network, packet transmission is easy, but achieving an effective routing path is difficult. The packet information is modified by the intruder node. Initial node capacity is not monitored, so it does not filter out the individual status of each and every node in the routing path. It causes a network that utilizes more energy and minimum packet delivery ratio. This work has implemented the enhanced centrum path allotment-based shielded communication (ECSC) scheme to achieve the shielded packet broadcasting from the sender node to the destination node in the network environment. The quality of packet transmission is improved by using the spatial uniqueness node selection algorithm. It is designed to select the routing node based on its uniqueness; priority-based communication is carried out by the uniqueness process. It improves the packet delivery ratio and network lifetime. It also minimizes packet drop rate and end-to-end delay.

## 1. Introduction

Sensors nodes should be newly applied in a network environment. This network is an identity configuring group of constant sensor nodes linked by two-way radio associates; anywhere, the nodes contain incomplete capability, storage space, and battery level. The location of sensor nodes should not be a constant, construction operation of a wireless sensor

network and a problem of concern [1]. There are amount of processes that converse wireless sensor network arrangement. According to the behavior, ensuring that wireless sensor networks are resistant to damage necessitates network techniques that obtain support nodes or alternative routes to base station nodes. It should require a better constructed sensor network arrangement in order to ensure a quantity of evaluate of strength in the network for those

communication techniques to continue to provide dependable transmission while packet drop is made [2].

Dependable communication schemes and techniques for monitoring packet dropping are presented, with the exception which is successful that forward on network techniques which ensure the convenience of another route to the base station node. Centrality is an important method in normal network monitoring [3]. This is applied to describe the significance of a node behavior in a network such as wireless sensor network environment. Fundamentally, it is considered by estimating the amount of minimum route distance which passes through a convinced node in network [4].

Previously different centrality indices are applied in network, containing nearest for central node, amount central node, worry central node, and connection-based central node. Those information are previously obtainable [5], distance between each node is measured [6], then route central nodes are mentioned, and its difference of minimum distance route among each node is analyzed. The distance between intermediate nodes is unbendable by the number of nodes neighbouring the sender node. The nearest relay node is an opposite amount of distance from sender node to each remaining nodes in network. Distance between immediate neighbour nodes provides an achievable centrality that determines a node's significance for its coverage limits in a network [7].

This routing path selection based on intermediate node in network environment for right to use indicates network operation and determines connection difficulty. Furthermore, intermediate relay node is used for communication and traffic controlling in the wireless sensor network environment [8]. The efficient path discovering is a vital characteristic of sensor network creation. Path optimization is used for finding optimum paths from the sender node to the destination node which considers available resources. The link established between sensor nodes from the standpoint of sender calculus obtains a recent technique for the survey of effective operation in a sensor network environment. It is used to reduce route issues in communication among sensor nodes in network environment [9].

A significant challenge issue for exposure is used to build sensor obstacles whose distance is covered by the sensor nodes in a barrier that can produce a permanent barrier that allows wireless sensor networks to detect attempts at entry amid the barrier or incisive guarded area. In the remaining sectors, blockade coverage is used in conjunction with reporting to increase the likelihood where attacks will be detected together with diffusion during the difficulty of the sensor, which also lowers the need for human hold. Freshly, barrier coverage has concerned additional uses [10, 11]. To identify packet information misuse by intruder nodes, the packet drops in the network environment and will have potential damage on each route from the sender to the target node. The method's main goal is to recognise attackers as they cross a shielded area or an irritated boundary [12].

The remaining part of the paper is designed as follows. Part II provides a related works. In Part III, we present the details of proposed enhanced centrum path allotment-based shielded communication (ECSC) technique that achieves the

centrum path; this path contains only spatial uniqueness nodes to improve network lifetime. Part IV provides simulation performance result analysis obtained under various metrics. Lastly, Part V concludes the paper with future direction.

## 2. Related Works

Brar and Gurbinder Singh et al. [13] offered a new way by merging the undefined route key worry with processing techniques for the common genuine group-based solution concern. For that time instance, it obtains capable set key conformity and organization by hierarchical depending addition of node matrix composition key exchange technique. Hypothetical analysis reveals that the latest approach has improved performance and achieves security and secrecy for sensor to launch several forms of key which distinguish from the current way.

Archana et al. [14] presented a transport method known as DTSN, in terms of throughput, connectivity, and storage rate, the best presentation is firm. Experimental output monitors show that when there was packet loss in the sensor network, relay node storing was able to do a great deal. However, the number of information transfer initiates that are made must fit into the description. When link argument is reached at a maximum transmission range and storage size of numbers, then for the buffer traffic rate, it is obtained at a minimum transmission range but with more storage space; correspondingly, these are the most suitable storing features. The connection which is recognized can hand out as a base for just beginning intrusion rate organization.

The established link can serve as the foundation for an early intrusion rate organisation in a sensor network using packet storage.

Rault. T et al., [15] provided a fast, adaptable, and energy-efficient multipath multirouting technique for data structuring. The basketball net technique, which maintains numerous links between sender and intermediate nodes in routing tables at all nodes, is suggested in the survey. Each node is also given a different accepted route before the intermediate nodes in order to eliminate broadcast intrusion. When packet transmission is divided into tasks, the distributed iterative preparation portion and time slot-based packet broadcasting are indicated. The entire wireless sensor network sequentially determines if a node must share a data packet to the destination; additionally, a child node must accept the data at the appointed time. The results of the experiment shows that the method can achieve low energy consumption and low traffic volume.

In [16], the authors presented the new tree-based method that is being used which is called DEACP, or dispersed energy wee-organized adaptive grouping method with data gathering, and it is intended for use in wireless sensor network environments. It is essential to increase dependability and extend the network's lifespan since sensor network nodes have insufficient energy. This strategy is used to reduce network energy consumption overall, stabilize energy consumption between sensor nodes, and lengthen

the lifespan of the network. The grouping must be dispersed, the grouping is effective in packet transmission challenges, and time slot allocation requires the group heads to be evenly distributed throughout the network.

In [17], they proposed a dispersed preparation algorithm for time slot-based packet transmission. A condition-based algorithm is applied for preparation, and its presentation is estimated. In order to personalize the preparation process for an incursion from a wireless network that uses a comparable spectral area environment, charitable consideration is placed in that network. Investigating wavelet packets depends on the path superiority inference. The experimental output of the present method indicates that the better scheduling efficiency is compared with the existing method.

The authors in [18] developed a technique to mitigate node damages caused by energy loss in a sensor network environment by selecting a subsequent neighbor node in light of a failed node. The current way of route repair is overload against it, resulting in the most effective use of energy for communication and extending the life of the network. Additionally, it results in the efficient exploitation of the important data packets at the entity nodes.

The authors in [19] presented TSSRM (trust sensing-based secure routing technique); it has the least amount of overhead and the ability to thwart numerous common intrusions that are present in this network simultaneously. At the same time, the protected path choosing method is effective by incorporating secure quantity and quality of service parameters into the description. The experimental output indicates that the TSSRM must enhance the protection and efficiency of the wireless sensor network.

In [20], the authors offered a different path to the conclusion that nodes are created in a more effective network. A network strategy that uses the operative calculus method to determine the efficient paths for all nodes to the target node is necessary for evaluating a recent metric. The current approach obtains two restrictions for all nodes into the description in order to characterize the network's path status, including energy and a BER-bit error rate. The simulation result indicates an enhanced presentation like the transmission rate and network lifespan.

### 3. Overview of Proposed Scheme

Sensor network contains a huge amount of sensor node that monitors the real-time network environment. Routing nodes have different characteristics; they are difficult to perform a similar kind of packet transmission from the source node to the destination node. The intermediate node selection is also vital, because poor characteristic nodes make the imperfect packet transmission. Destination node organizes data packets normally without distortion; it reduces the packet drop made in the intermediate node. So it does not perform shielded packet transmission.

Figure 1 shows the proposed enhanced centrum path allotment-based shielded communication technique that obtains better routing; it only allows to broadcast shielded data packets. Normal sensor establishes a communication with unshielded packet that is avoided by using this scheme.

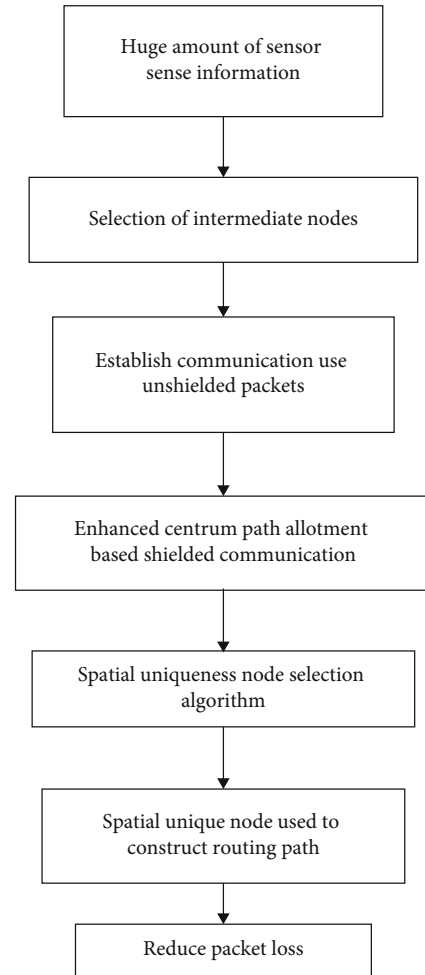


FIGURE 1: Block diagram of enhanced centrum path allotment-based shielded communication technique.

Spatial uniqueness node selection algorithm is constructed; it selects the node which has high spatial uniqueness capacity. It uses a spatial unique node for communication in particular routing path, and then it improves packet delivery ratio and minimizes packet drop rate.

The present enhanced centrum path allotment-based shielded communication (ECSC) method allows shielded packet transmission along the centrum routing path. Every time the communication dependability is checked, if the reliability rate is low, information is lost or blocked; otherwise, if the reliability rate is high, there is no packet loss. The spatial uniqueness node selection algorithm separates the sensor node which has a spatial unique behavior which analyzes various nodes and chooses the spatial node as a relay node. This scheme reduces packet drop rate and time delay.

*3.1. Sensor Node Establishes Communication Use Unshielded Packets.* A source node should contain lot of intermediate nodes. Whether two or more intermediate nodes are irritating to broadcast information to the unwanted node that are available in out of route, then packet drop is made [21]. Due to the fact that each intermediate node does not have a comparable amount of information to broadcast, it is uncertain

for a sender node to guarantee a permanent time slot allocation to all of its intermediate nodes. As a result, a time slot is allocated for all intermediate nodes that are present in the routing path to broadcast packets to the required destination node [22]. Time slot allocation for these methods, which accept all nodes to incorporate adaptive packet forwarding, is dependent on path overload. Take into account that communication is  $C$ , unshielded data packets are  $US$ , and time slot  $T$ .

$$C = US(D_p) * T. \quad (1)$$

The time slot allocation process rejects the packet loss made by intermediate relay nodes broadcast data packet to the similar destination node frequently. While a node broadcasts a data packet to the destination node, packet loss occurs continually; however, overloading occurs when all of the intermediary nodes can accept the packet [23]. For extra, the attacker node issues should make the packet loss in an intermediate node. Although a node should broadcast the data packet to the intermediate node, when it gets many data packets at once, the node produces overload. Regardless of whether the destination node attempts to broadcast a packet at a specific moment, the packet loss takes place in an intermediate node. So once more, in a wireless context, broadcasting the same information to the destination node  $S \leftrightarrow R$  is a source node to the relay node:

$$US(D_p) = S \leftrightarrow R + SU. \quad (2)$$

Consequently, the multipath scheme is used to perform a process to hand out the remaining intermediate nodes in a sequence manner to reject attack and packet overload. Each node should contain its individual route path selection. These paths should not have similar intermediate nodes with the route path sender node for intermediate nodes. Each intermediate node has the ability to identify the sender node's path. The target node should have a link to the intermediate node's routing path even though the intermediate node must broadcast data packets to its destination node. A procedure to broadcast a data packet to the destination node should be started by the intermediate node, and the destination node should also receive those information packets [23]. Packet broadcasting from the sender to the destination node occurs as part of the multipath procedure. Throughout packet broadcasting, all nodes should be in control of the path to their destination node and should refuse interference from other nodes. Control is then granted to the source node's routing path following the data broadcast by that node.

$$S \leftrightarrow R = S \rightarrow \frac{R}{S} \leftarrow R. \quad (3)$$

The grouping of multipath separation and time period assigned is used to obtain an intrusion liberated packet sharing. Since the path is open for packet broadcasting, the multipath separation rejects incursion from all remaining nodes, and the time slot allocation prevents multiple inter-

mediate nodes from simultaneously broadcasting data packets to the same target node. Consequently, the time slot period can be smart to the time of broadcasting single data packet with the time of holding for reply message.

*3.2. Enhanced Centrum Path Allotment-Based Shielded Communication.* Firstly, the destination node broadcasts a request packet to the intermediate nodes within its coverage area. The delivery of the target node's request packet and a reply packet are sent to each accepting node, which also becomes the target node's intermediate node. Consider target node range as the bare minimum, and this collection of intermediate nodes as recognised above range yet another [24]. All nodes at range one broadcast request message to the nearest neighbor node. For condition, a node that does not establish its destination node should accept request packets from more than one node. Currently, every node finds the neighbour node wherever it is; it contains the request packet and confirms that it came from the sender node.

$$S \rightarrow R = Sreq \rightarrow Rreq. \quad (4)$$

Once the request packet is accepted by each of the network's remaining nodes, alternate sender nodes should be used. These exchanges take place often in the sensor network to gather all the ranges and turn over the creation of the entire path. Consider that all nodes contain the detail about the sender, receiver, and also neighboring node with network overload. The sake of brevity in this process must launch the initial route allocation scheme. In order to collect all the ranges and turn over the creation of the full path, these exchanges occur frequently in the sensor network. A node establishes a process hold that is carried out by each node in the network environment. A crucial assumption is that the network's traffic is distributed equitably through sensor nodes according to outside uncertainty.

$$\begin{aligned} S \leftarrow R &= Sreq \leftarrow Rreq, \\ S \leftrightarrow R &= Sreq \rightarrow \frac{Rreq}{Sreq} \leftarrow Rreq. \end{aligned} \quad (5)$$

All nodes frequently analyze its power usage and accessibility. Execute the process by all nodes to obtain efficient communication. The energy level of a node attains the energy threshold value; it notifies to its neighbor nodes to appear for the latest next sender to arrive at the target node. The sender node initiates this communication at each of the nodes that should be external, instructs from its packet drop, and then watches for a recent sender node. The routing table contains the data of all neighbours searching for a recent sender node. In order to broadcast their traffic data and count the number of nodes, all nodes keeping track of their neighbours send the appropriate request packet to their complete next neighbour node. To identify alternate routing routes in case, any nodes are damaged.

$$US(D_p) = Sreq \rightarrow \frac{Rreq}{Sreq} \leftarrow Rreq + SU. \quad (6)$$



By broadcasting the request data packets, accepting the request packet shall respond to the similar. Currently, the neighbor node monitoring for a next sender node chooses the most qualified optional sender node from its route, and it builds new sender node. Packet overload of the recent sender node must be lesser among the nodes in the network. The quantity of nodes to make the target node from the recent sender should be negligible:

$$T = Allotment - Delay. \quad (7)$$

Activate the neighbor node to choose the efficient optional sender node as its recent neighbor. Due to the importance of traffic and node amount in selecting the next neighbour node, act upon the resource range given to all of the aforementioned conditions. The simulation shows how the node's resources should be tied to its traffic and quantity, respectively. It is an efficient path which balances the traffic:

$$C = Sreq \longrightarrow \frac{Rreq}{Sreq} \longleftarrow Rreq + SU * Allotment - Delay. \quad (8)$$

In Algorithm 1, the enhanced centrum path allotment-based shielded communication allows shielded packet transmission along the centrum routing path. Every time the communication dependability is checked, if the reliability rate is low, and information is lost or blocked; otherwise, if the reliability rate is high, there is no packet loss.

**3.3. Spatial Uniqueness Node Selection Algorithm.** The node selecting method is applied to discover the effective nodes which consume a minimum energy in wireless sensor network. This method runs at the destination node and predicts that the operation will take less time overall depending on the range of packet loss. These details are sent to each sensor node together with an estimate of the typical distance between the sender node and the destination node. Each node's required mathematical resources are distributed as input packets. Choosing of position of each node should perform intrusion free packet transmission in a wireless sensor network. *SU* stands for spatial uniqueness and efficient path allocation.

$$SU = EP,$$

$$C = Sreq \longrightarrow \frac{Rreq}{Sreq} \longleftarrow Rreq + EP * Allotment - Delay. \quad (9)$$

Separating the sensor network allows for the discovery of the communication useful spatial uniqueness node. The position of the agent node is monitored, and it indicates the coverage range of all neighbor nodes. It chooses the node with the unique character, enabling continuous communication between sensor nodes. It gathers data from the surroundings and transmits it, selecting the node for spatial uniqueness along the way. Consequently, it offers the best route between the sender and the destination node.

```

Step1: Establish path from source to destination node
Step 2: for each find neighbor nodes
Step3: sense the information from real time environment
Step 4: if {node! = broadcast packet}
Step 5: Unshielded packet transmission
Step 6: else if {node == broadcast packet}
Step 7: Shielded packet transmission.
Step 8: End if
Step 9: if {Packet == shielded}
Step 10: Packet information not intruded
Step 11: else if {Packet! = shielded}
Step 12: Packet information is intruded.
Step 13: End if
Step 14: End for

```

ALGORITHM 1: Enhanced centrum path allotment-based shielded communication.

```

Step 1: Monitor node behavior of entire network
Step 2: Select routing path
Step 3: if {node == Spatial uniqueness}
Step 4: select those node to perform communication.
Step 5: else if {node! = Spatial uniqueness}
Step 6: those nodes are removed.
Step 7: go to alternative nodes for routing.
Step 8: end if
Step 9: Reduce Packet drop rate
Step 10: Improve packet delivery ratio
Step 11: End for.

```

ALGORITHM 2: Spatial uniqueness node selection.

Sensor nodes do not provide the perfect packet transmission; Algorithm 2 introduces the spatial uniqueness node selection to separate nodes based on the performance. It improves packet delivery ratio and reduces packet loss rate. It controls the traffic rate for every packet broadcasting through the route from the source to the destination node.

The preceding and subsequent neighbour node performance information is contained in the packet ID. Neighbor node position and coverage limits are measured.

In Table 1, the proposed ECSC packet format is shown. Here, the source and destination node ID field take 4 bytes. The third one is the presence of enormous volumes of sensor detecting data, which takes up 4 bytes. Information is sensed by the sensor node's maximum count, and it is sent to the neighbouring node. The fourth field occupies 2 bytes. Established communication uses unshielded packets; it broadcasts the normal unshielded data packets frequently. The intermediate nodes with the highest capacity are chosen using enhanced centrum path allotment-based shielded communication in sixth uses 4 bytes. One final field is to minimize packet drop rate; a spatial uniqueness node selection algorithm is used to separate the nodes that support the features of spatial uniqueness that consumes 6 bytes.

TABLE 1: Proposed ECSC packet format.

Source ID	Destination ID	Huge amount of sensor sense information	Establish communication use unshielded packets	Enhanced centrum path allotment based shielded communication	Spatial uniqueness node selection algorithm
4	4	3	2	4	6

## 4. Performance Evaluation

**4.1. Simulation Model and Parameters.** The proposed ECSC is simulated with the network simulator tool (NS 2.34). In our simulation, 100 mobile nodes move in an 860-meter  $\times$  660-meter square region for 30 milliseconds simulation time. Each mobile node goes in a random manner among the network in different speeds. All nodes have the same transmission range of 250 meters. To reduce network traffic, CBR (constant bit rate) maintains a constant speed for packet transmission. Shielded packet transfer from the source node to the destination node is achieved using the AODV (ad hoc on-demand distance vector) routing protocol. Table 2 illustrates the estimation of the simulation setup.

**4.1.1. Simulation Result.** Figure 2 shows that the proposed ECSC technique obtains the better shielded packet transmission in routing path and is compared with the existing RTS [19] and NPC [20]. ECSC method provides an enhanced communication in sensor routing path. Spatial uniqueness node selection algorithm is introduced to discover the spatial uniqueness node; it only allows the shielded data packets from source node to destination node. Finally, it improves packet delivery ratio and reduces packet drop rate.

**4.2. Performance Analysis.** Utilizing the X graph in ns2.34 in simulation, the following performance metrics were examined.

**4.2.1. End-to-End Delay.** The end-to-end delay is depicted in Figure 3 as being determined by the time required for packet transmission from the source node to the destination; information about each node is kept in the routing table. Compared to the current methods RTS, CREPG, and NPC, the end-to-end delay is reduced in the proposed ECSC approach.

$$\text{End to End Delay} = \text{End Time} - \text{Start Time}. \quad (10)$$

**4.2.2. Network overhead.** Figure 4 demonstrates how the network overhead is reduced when a packet is sent from the sender to the receiver node. The algorithm for spatial uniqueness node selection chooses the distinctive nodes for network routing from the sender to the target node. Compared to the current methods RTC, CREPG, and NPC, the suggested ECSC approach has the least amount of network overhead.

$$\text{Network overhead} = \left( \text{Number of Packet} \frac{\text{Losses}}{\text{Received}} \right) * 100. \quad (11)$$

TABLE 2: Simulation setup.

No. of nodes	100
Area size	860 $\times$ 660
Mac	802.11 g
Radio range	250 m
Simulation time	30 ms
Traffic source	CBR
Packet size	512 bytes
Mobility model	Random way point
Protocol	AODV

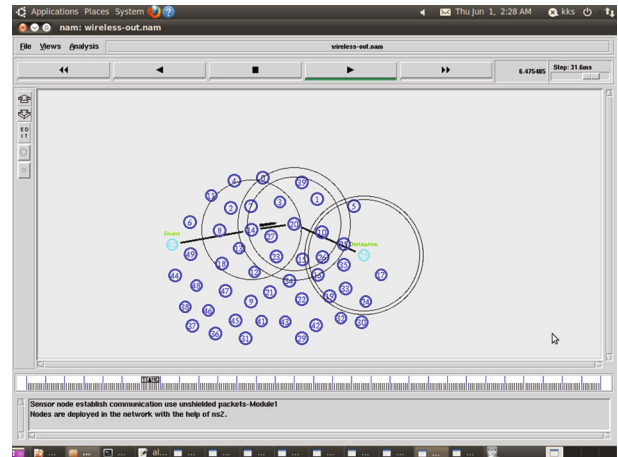


FIGURE 2: Proposed ECSC result.

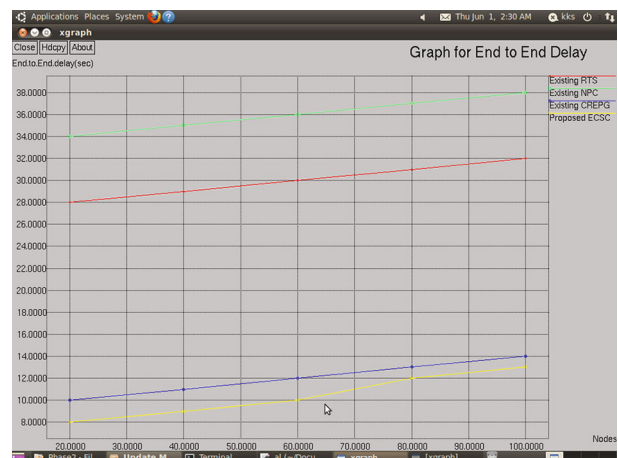


FIGURE 3: Graph for nodes vs. end-to-end delay.

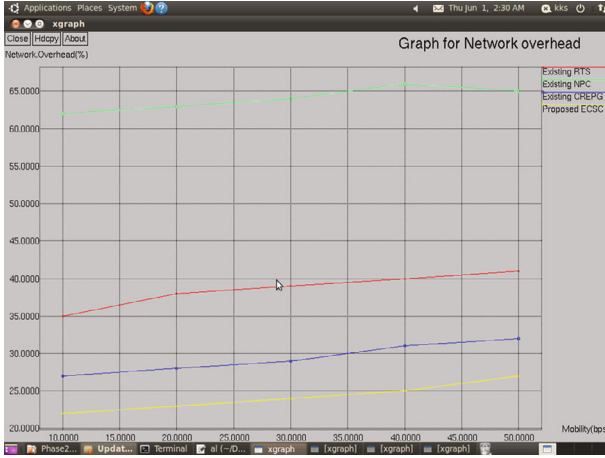


FIGURE 4: Graph for mobility vs. network overhead.

4.2.3. *Packet Delivery Ratio.* Figure 5 demonstrates how the number of packets received is calculated from the number of packets delivered at a specific speed. The node velocity is not a constant; simulation mobility is fixed at 100 (bps). In the proposed ECSC method, the packet delivery ratio is increased compared to the existing method RTS, CREPG, and NPC:

$$\text{Packet Delivery Ratio} = \left( \text{Number of packet} \frac{\text{received}}{\text{Sent}} \right) * \text{speed}. \quad (12)$$

4.2.4. *Connectivity ratio.* Figure 6 shows the connectivity ratio; the weak connectivity between the nodes in the routing path is removed by the spatial uniqueness node selection algorithm to monitor characteristics and split the spatial uniqueness node from the network environment. In the proposed ECSC method, the connectivity ratio is improved compared to the existing method RTS, CREPG, and NPC:

$$\text{Connectivity ratio} = \frac{\text{weak connection}}{\text{overall connection}}. \quad (13)$$

4.2.5. *Energy.* Figure 7 depicts energy usage and the total amount of energy spent on communication, which is calculated from the energy consumption's beginning level to its conclusion. In comparison to the current methods RTS, CREPG, and NPC, the proposed ECSC technique achieves a shielded communication path to select higher spatial uniqueness nodes from the sender to the destination node.

$$\text{Energy Consumption} = \text{Initial Energy} - \text{Final Energy}. \quad (14)$$

4.2.6. *Packet loss.* Figure 8 shows that the packet loss of particular communication in network is calculated by node loss packet with weak connectivity to obtain efficient transmission; the unwanted node characteristics are monitored and removed by using spatial uniqueness node selection algorithm. In the proposed ECSC method, packet loss is reduced compared to the existing method RTS, CREPG, and NPC:

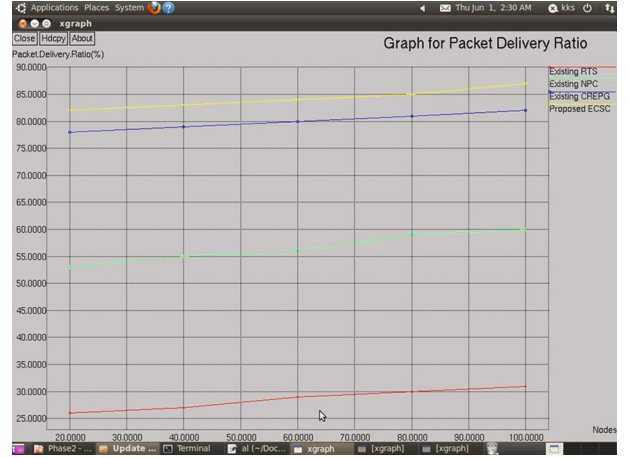


FIGURE 5: Graph for nodes vs. packet delivery ratio.

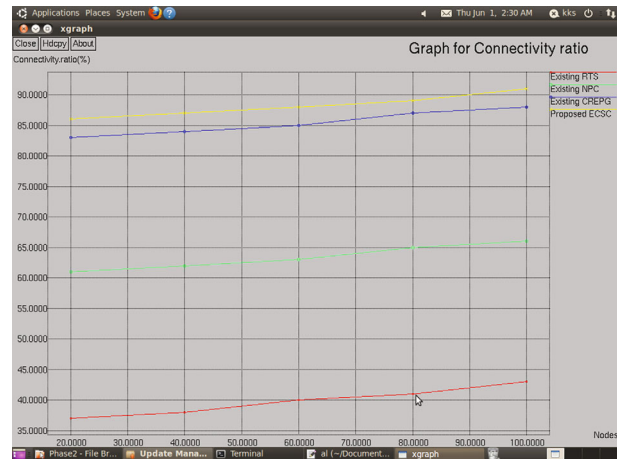


FIGURE 6: Graph for nodes vs. connectivity ratio.

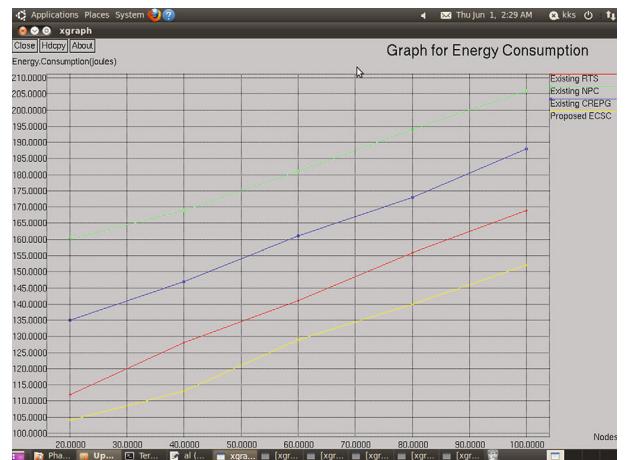


FIGURE 7: Graph for nodes vs. energy consumption.

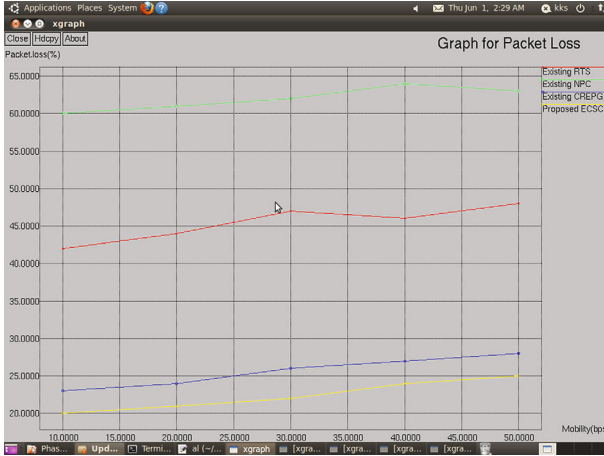


FIGURE 8: Graph for mobility vs. packet loss.

$$\text{Packet loss} = \left( \text{Number of packet} \frac{\text{dropped}}{\text{Sent}} \right) * 100. \quad (15)$$

## 5. Conclusion

Sensor node communication is difficult because it broadcast data packet in unshielded information from sender node to destination node. The unwanted nodes are available in routing that wrongly transmits the unshielded data packets and misuse, so packet delivery rate is reduced. Route path breakage makes the packet drop in routing. So, proposed enhanced centrum path allotment-based shielded communication (ECSC) technique is used to obtain shielded communication; the packets are safely covered before transmission initiated, and then it broadcasts the data packets in continuous manner; spatial uniqueness node selection algorithm is construct; it selects the node which has high spatial uniqueness capacity, and then it improves packet delivery ratio and minimizes packet drop rate.

Future improvements will include non-uniqueness and data optimization approaches for safe data. Node obtains steady communication and also does various parameter analyses.

## Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

## Conflicts of Interest

There is no conflict of interest.

## References

- [1] D. Bri, M. Garcia, J. Lloret, and P. Dini, "Real deployments of wireless sensor networks," in *Third International Conference on Sensor Technologies and Applications (SENSORCOMM'09)*, Athens/Glyfada, Greece, 2009.
- [2] S. Zhu, C. Chen, and X. Guan, "Sensor deployment for distributed estimation in heterogeneous wireless sensor networks," *Ad Hoc and Sensor Wireless Networks*, vol. 16, no. 4, pp. 297–322, 2013.
- [3] I. Boulanouar, S. Lohier, A. Rachedi, and G. Roussel, "DTA: deployment and tracking algorithm in wireless multimedia sensor networks," *Ad Hoc and Sensor Wireless Networks*, vol. 28, no. 1-2, 2015.
- [4] M. Garcia, D. Bri, S. Sendra, and J. Lloret, "Practical deployments of wireless sensor networks: a survey," *International Journal on Advances in Networks and Services*, vol. 3, no. 1-2, pp. 163–178, 2010.
- [5] N. Meghanathan and P. Mumford, "Centralized and distributed algorithms for stability-based data gathering in mobile sensor networks," *Network Protocols and Algorithms*, vol. 5, no. 4, pp. 84–116, 2013.
- [6] R. P. Anand and A. Rajaram, "Effective timer count scheduling with spectator routing using stifle restriction algorithm in manet," *IOP Conference Series: Materials Science and Engineering*, vol. 994, no. 1, article 012031, 2020.
- [7] J. Jiang, G. Han, H. Guo, L. Shu, and J. J. P. C. Rodrigues, "Geographic multipath routing based on geospatial division in duty-cycle underwater wireless sensor networks," *Journal of Network and Computer Application*, vol. 59, pp. 4–13, 2016.
- [8] Y. Shavitt and Y. Singer, "Beyond centrality-classifying topological significance using backup efficiency and alternative paths," *New Journal of Physics*, vol. 9, no. 8, p. 266, 2007.
- [9] A. Cuzzocrea, A. Papadimitriou, D. Katsaros, and Y. Manolopoulos, "Edge betweenness centrality: a novel algorithm for QoS-based topology control over wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1210–1217, 2012.
- [10] S. Kannan and A. Rajaram, "QoS aware power efficient multicast routing protocol (QoS-PEMRP) with varying mobility speed for mobile ad hoc networks," *International Journal of Computer Applications*, vol. 60, no. 18, pp. 15–19, 2012.
- [11] A. Plutov and M. Segal, "The Delta-Betweenness Centrality," in *IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 3376–3380, London, UK, 2013.
- [12] T. Alahakoon, R. Tripathi, N. Kourtellis, R. Simha, and A. Iamnitchi, "K-path centrality: a new centrality measure in social networks," in *Proceeding of the 4th Workshop on Social Network Systems (SNS)*, pp. 1–31, Salzburg, Austria, 2011.
- [13] U. Brandes, "On variants of shortest-path betweenness centrality and their generic computation," *Social Networks*, vol. 30, no. 2, pp. 136–145, 2008.
- [14] L. Sitanayah, K. Brown, and C. Sreenan, "Fault-tolerant relay deployment based on length-constrained connectivity and rerouting centrality in wireless sensor networks," in *Wireless Sensor Networks. EWSN 2012*, G. P. Picco and W. Heinzelman, Eds., vol. 7158 of Lecture Notes in Computer Science, pp. 115–130, Springer, Berlin, Heidelberg, 2012.
- [15] W. An, S. Ci, H. Luo et al., "Overall cost minimization for data aggregation in energy-constrained wireless sensor networks," in *2013 IEEE International Conference on Communications (ICC)*, Budapest, Hungary, 2013.
- [16] T. Rault, A. Bouabdallah, and Y. Challal, "WSN lifetime optimization through controlled sink mobility and packet buffering," in *Global Information Infrastructure Symposium - GIIS 2013*, Trento, Italy, 2013.



- [17] R. P. Premanand and A. Rajaram, "Enhanced data accuracy based PATH discovery using backing route selection algorithm in MANET," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2089–2098, 2020.
- [18] A. Rajaram and S. Palaniswami, "Malicious node detection system for mobile ad hoc networks," (*IJCSIT International Journal of Computer Science and Information Technologies*, vol. 1, no. 2, pp. 77–85, 2010.
- [19] F. Ren, J. Zhang, T. He, C. Lin, and S. K. D. Ren, "EBRP: energy-balanced routing protocol for data gathering in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 12, pp. 2108–2125, 2011.
- [20] D. Vukobratovic, C. Stefanovic, V. Crnojevic, F. Chiti, and R. Fantacci, "Rateless packet approach for data gathering in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 7, pp. 1169–1179, 2010.
- [21] A. K. Yogi and J. Surana, "An implementation of modified AOMDV routing protocol in different wireless networks," in *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, India, 2016.
- [22] S. Yang, U. Adeel, Y. Tahir, and J. A. McCann, "Practical opportunistic data collection in wireless sensor networks with mobile sinks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 5, pp. 1420–1433, 2017.
- [23] M. Hammoudeh, F. al-Fayez, H. Lloyd et al., "A wireless sensor network border monitoring system: deployment issues and routing protocols," *IEEE Sensors Journal*, vol. 17, no. 8, pp. 2572–2582, 2017.
- [24] S. Palaniswami and A. Rajaram, "An enhanced distributed certificate authority scheme for authentication in mobile ad hoc networks," *The International Arab Journal of Information Technology (IAJIT)*, vol. 9, no. 3, pp. 291–298, 2005.