International Journal of Emerging Research in Engineering, Science, and Management
Vol. 5 | Issue 1 | pp. 93-106 | Jan-Mar 2026.
www.ijeresm.com | eISSN – 2583-4894
Received: 29 Dec 2025 | Revised: 14 Mar 2026 | Accepted: 21 Mar 2026 | Published: 30 Mar 2026

Backward Token-Based Routing Framework for Hierarchical Tree Construction and Collision-Controlled Transmission in Wireless Sensor Networks

[1]S Navaneethan, [2]A Arun*

[1]Research Scholar, [2]Associate Professor
Department of Networking & Communications, School of Computing, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Chengalpattu District, Tamil Nadu - 603203, India.
[1]ns2066@srmist.edu.in | ORCID: 0009-0005-2379-7176, [2]aruna2@srmist.edu.in | ORCID: 0000-0002-6174-2468

*Corresponding Author: A Arun

Abstract: Wireless Sensor Networks (WSNs) require efficient routing mechanisms to ensure reliable data delivery while minimizing energy consumption and communication delay in resource-constrained environments. Conventional methods, including contention-based transmission schemes, often suffer from packet collisions, retransmissions, and increased latency as network density mounts. To combat these challenges, this paper proposes a Backward Token-Based Routing Framework (BTBRF) that allows a sink-initiated reverse-direction token propagation for hierarchical routing tree construction and controlled transmission scheduling in multi-hop WSN structures. In the proposed approach, backward tokens are generated at the sink node and establish parent–child relationships using hop count, path cost, and residual energy metrics. This ensures loop-free topology formation and regulated channel access. Hence, only authorized nodes participate in communication at a given time. The performance of the proposed framework was evaluated using the QualNet network simulator by varying node densities from 20 to 100 nodes. Simulation results demonstrate that the proposed method improves packet delivery ratio and throughput while reducing end-to-end delay and overall energy consumption compared with conventional single-token communication methods.

Keywords: Wireless Sensor Networks, Token-Based Routing, Backward Token Propagation, Energy-Efficient Routing, Hierarchical Routing Tree, Collision-Controlled Transmission, QualNet Simulation, Packet Delivery Ratio.

1 INTRODUCTION

Wireless Sensor Networks are widely positioned in distributed sensing environments where battery-powered nodes must forward measurements over multiple hops toward a centralized sink. Because communication dominates energy consumption in such networks, routing coordination and transmission scheduling remain critical design challenges. A typical WSN consists of a large number of energy-constrained sensor nodes that collaboratively collect information from the physical environment and transmit it to a sink node for further processing. Because sensor nodes operate with limited battery resources and short communication ranges, efficient routing and medium access coordination mechanisms are essential for improving network lifetime and ensuring reliable data delivery.

Cluster-based routing protocols such as Low-Energy Adaptive Clustering Hierarchy (LEACH) have been widely used to improve energy efficiency by rotating cluster-head responsibilities among sensor nodes and reducing long-distance transmissions toward the sink node [1]. Similarly, chain-based routing approaches such as PEGASIS organize nodes into linear communication structures to minimize transmission overhead and extend network lifetime through multi-hop forwarding [2]. Data-centric routing techniques, including Directed Diffusion, enable attribute-based data dissemination using query-driven communication mechanisms that improve reliability in dynamic wireless environments [3]. In addition, hybrid energy-aware clustering protocols such as HEED select cluster heads based on residual energy and communication cost metrics to achieve balanced energy consumption across the network [4].

One of the major challenges in multi-hop WSN communication is channel contention among sensor nodes attempting to transmit data simultaneously. Contention-based medium access mechanisms often lead to packet collisions, retransmissions, increased delay, and higher energy consumption. These issues become more significant as the network size increases or the traffic load grows. Therefore, controlled transmission scheduling mechanisms that regulate node participation during communication can significantly improve network performance. Token-based communication approaches have been widely investigated in wireless networks as an effective solution for reducing contention and improving channel utilization.

https://doi.org/10.58482/ijeresm.v5i1.8

Token-controlled scheduling mechanisms allow nodes to access the communication channel only when transmission permission is granted, thereby reducing collisions and improving throughput performance. For example, token-based scheduling techniques have been proposed to support prioritized traffic transmission and improve channel utilization in wireless local area networks (WLANs) [5]. Similarly, token-ring-based approaches have been explored for providing predictable channel access and quality-of-service support in ad-hoc wireless networks [6]. Middleware-level token coordination mechanisms have also been investigated to enhance deterministic communication performance over IEEE 802.11-based industrial wireless systems [7].

In addition to medium access coordination, token-assisted communication techniques have been applied in monitoring applications and wireless sensor environments to enable orderly transmission among distributed sensing nodes [8]. Token-based mechanisms have also been used in secure wireless communication systems to support authentication and payload integrity protection [9], [10]. These studies demonstrate that token-controlled communication can significantly improve transmission reliability and coordination efficiency in distributed wireless environments. Despite these advantages, most existing token-based mechanisms operate primarily at the medium access control layer or within logical ring-based communication structures. Such approaches are not directly suitable for hierarchical routing tree construction in large-scale multi-hop WSN deployments. In particular, existing methods typically employ forward token circulation or ring-based token propagation rather than sink-initiated reverse-direction token dissemination for topology discovery and routing coordination.

To address these limitations, this paper proposes a Backward Token-Based Routing Framework for efficient data transmission in wireless sensor networks. In the proposed approach, the sink node periodically generates backward tokens that propagate toward leaf nodes to establish parent–child relationships based on hop count, path cost, and residual energy metrics. The backward token mechanism enables controlled channel access in which only token-authorized nodes participate in transmission at a given time, thereby reducing contention and improving packet delivery reliability. The major contributions of this work are summarized as follows:

- Sink-initiated backward token propagation enables hierarchical routing-tree construction
- Parent selection combines hop distance, path cost, and residual node energy
- Token-regulated transmission scheduling limits simultaneous channel access
- Loop-free topology formation is maintained using monotonic hop-count constraints
- Performance is validated through QualNet-based simulation across multiple node densities

The remainder of this paper is organized as follows. Section 2 presents the related work on token-based communication mechanisms in wireless networks. Section 3 describes the proposed backward token-based routing framework. Section 4 discusses the simulation setup and performance evaluation. Section 5 presents results and discussion, followed by conclusions in Section 6.

2 RELATED WORK

Token-based communication mechanisms have been widely studied as an effective approach for improving channel access coordination and transmission efficiency in wireless networks. These mechanisms regulate medium access by granting transmission permission only to nodes holding a valid token, thereby reducing contention and improving reliability in distributed communication environments. Token-controlled scheduling techniques have been investigated for wireless local area networks to support prioritized transmission and service differentiation among traffic classes. Wang and Zhuang proposed a token-based scheduling scheme that improves channel utilization and reduces contention overhead compared with conventional contention-based approaches [5]. Similarly, middleware-level token coordination mechanisms were introduced to enhance deterministic communication performance over IEEE 802.11-based wireless systems, demonstrating improved delay performance under real-time traffic conditions [7].

Token-ring-based communication structures have also been explored in wireless ad-hoc environments to provide predictable medium access and quality-of-service support. Narasimhan and Deepa proposed a distributed token-ring-based approach for QoS provisioning in ad-hoc networks, showing improved response time for real-time data transmission compared with conventional contention-based methods [6]. Likewise, token-ring-based communication frameworks have been applied in distributed sensing applications to enable orderly data sharing among participating wireless nodes [8].

In addition to channel access coordination, token-based mechanisms have been investigated for improving communication security in wireless environments. Abduljabbar et al. proposed a session-dependent token-based payload enciphering scheme that enhances communication integrity and privacy in wireless sensor systems [9]. Similarly, Cui et al. introduced a biometric-enhanced token-based key derivation framework for secure authentication in wireless networks [10]. Although these approaches improve communication security, they do not address routing topology formation or energy-efficient packet forwarding in WSN environments. Several studies have also investigated token-passing mechanisms for reservation-based communication protocols and dynamic token-ring network coordination to improve transmission efficiency in distributed wireless systems [11], [12]. These approaches demonstrate the effectiveness of token-controlled communication for reducing contention and improving transmission coordination.

However, token propagation in these frameworks typically follows forward transmission direction or logical ring-based circulation patterns rather than sink-initiated reverse topology discovery for routing tree construction. From the above discussion, it can be observed that existing token-based communication approaches mainly focus on medium access scheduling, logical ring formation, or communication security enhancement. The use of sink-initiated backward token propagation for hierarchical routing tree construction and controlled data transmission scheduling in multi-hop WSN environments has not been adequately investigated. Although clustering-based routing protocols such as LEACH, chain-based routing approaches such as PEGASIS, data-centric routing techniques such as Directed Diffusion, and hybrid clustering frameworks such as HEED improve energy efficiency and communication reliability in wireless sensor networks, these approaches primarily rely on periodic clustering, chain formation, or attribute-based forwarding mechanisms rather than token-assisted topology discovery and transmission scheduling.

These routing strategies do not incorporate sink-initiated backward token propagation for hierarchical routing tree construction and controlled medium access coordination. To address this research gap, this paper proposes a backward token-based routing framework that enables reverse-direction topology discovery and collision-controlled transmission scheduling using token-authorized communication paths. The proposed approach integrates token-assisted routing tree formation with energy-aware parent selection to improve packet delivery reliability and reduce communication overhead in dense wireless sensor network deployments.

Table 1. Comparison of Token-based Communication Mechanisms

Method	Category	Token Direction	Routing Strategy	Energy Awareness	Collision Control	Routing Tree Formation	Suitable for Multi-hop WSN
LEACH routing protocol [1]	Cluster-based routing	Not applicable	Cluster-head rotation	Yes	Partial	Cluster-based	Yes
PEGASIS routing protocol [2]	Chain-based routing	Not applicable	Linear chain forwarding	Yes	Partial	Chain-based	Yes
Directed Diffusion routing [3]	Data-centric routing	Not applicable	Attribute-based forwarding	Partial	No	Query-driven	Yes
HEED routing protocol [4]	Hybrid clustering routing	Not applicable	Energy-aware clustering	Yes	Partial	Cluster-based	Yes
Token-based WLAN scheduling [5]	MAC scheduling	Forward	Channel access scheduling	No	Yes	No	No
QoS Token-ring (Ad-hoc networks) [6]	Token ring MAC	Circular	Logical ring structure	Partial	Yes	No	Limited
Token middleware over IEEE 802.11b [7]	Middleware coordination	Forward	Deterministic access control	No	Yes	No	No
Wireless token-ring sensing system [8]	Token ring sensing	Circular	Ring-based sensing coordination	No	Yes	No	Limited
Token-based payload enciphering [9]	Security framework	Session-based	Secure communication	No	No	No	No
Biometric token authentication [10]	Security framework	Session-based	Authentication support	No	No	No	No
Reservation-based token passing protocol [11]	MAC coordination	Forward	Reservation scheduling	No	Yes	No	No
Dynamic token-ring coordination [12]	Token ring MAC	Circular	Adaptive ring coordination	No	Yes	No	No
Proposed BTBRF	**Routing + token scheduling**	**Backward (Sink → Nodes)**	**Hierarchical routing tree**	**Yes**	**Yes**	**Yes**	**Yes**

The comparison presented in Table 1 shows that most existing token-based communication mechanisms operate either at the medium access control layer or within logical ring-based communication structures and are not designed for hierarchical routing tree construction in multi-hop wireless sensor networks.

3 PROPOSED BACKWARD TOKEN-BASED ROUTING FRAMEWORK

This section describes the proposed BTBRF for efficient data transmission in Wireless Sensor Networks. The framework constructs a hierarchical routing tree using a sink-initiated backward token mechanism that enables controlled channel access, collision reduction, and energy-aware parent selection. The proposed method operates in three main phases:

1. Backward Token Generation Phase
2. Routing Tree Construction Phase
3. Token-Controlled Data Transmission Phase

3.1. Network Model Constraints

The following constraints are considered for the proposed framework:

- Sensor nodes are randomly deployed in a 500 × 500m² sensing area (This deployment size represents a typical medium-scale environmental monitoring scenario frequently adopted in WSN simulation studies.)
- Nodes remain static after deployment
- All nodes are energy-constrained
- Sink node has unlimited energy resources
- Nodes communicate using the IEEE 802.15.4 MAC protocol
- Transmission follows the Two-Ray Ground propagation model
- Initial node energy is 1 Joule
- Packet size is 128 bytes
- Traffic model is Constant Bit Rate (CBR)

3.2. Backward Token Generation Phase

The sink node periodically generates a Backward Token (BT) that propagates through the network toward leaf nodes using multicast tree-based dissemination. The backward token contains routing information required for topology construction:

$$BT = \{TokenID, SourceID, ParentID, HopCount, ResidualEnergy, SequenceNumber\} \quad (1)$$

Each receiving node performs the following operations:

1. Updates hop count
2. Computes path cost
3. Evaluates parent eligibility
4. Registers routing information
5. Rebroadcasts the token

The hop count is updated as:

$$HopCount_i = HopCount_j + 1 \quad (2)$$

Each node selects the minimum hop-count path toward the sink:

$$HopCount_i = \min\,(HopCount_j + 1) \quad (3)$$

Because hop count monotonically decreases toward the sink, routing loops are avoided automatically.

3.3. Parent Node Selection Mechanism and Path Estimation

Each node selects its parent node using a weighted multi-parameter decision function:

$$P_i = \arg\ \min\left(w_1 \cdot HopCount_j + w_2 \cdot PathCost_j - w_3 \cdot Energy_j\right) \quad (4)$$

where $HopCount_j$ is represents the hop distance from the sink node, $PathCost_j$ is the routing transmission cost, $Energy_j$ is residual energy, w_1 is hop-count weight (0.5), w_2 is path-cost weight (0.3), and w_3 is energy weight (0.2). These coefficients were selected after evaluating multiple combinations during pilot simulations to avoid excessive parent switching while preserving energy-balanced routing paths. This ensures that routing decisions prioritize:

- shortest distance to sink
- minimum transmission cost
- higher residual energy

leading to balanced energy utilization across the network. Path cost is computed using both distance and residual energy:

$$PathCost_i = PathCost_j + \alpha d_{ij} + \beta \frac{1}{E_j} \tag{5}$$

where d_{ij} is the Euclidean distance between nodes, α is the distance weight (0.6), and β is the energy weight (0.4). This formulation ensures that nodes with shorter distances and higher residual energy are preferred during route formation.

3.4. Residual Energy Model

The proposed framework adopts the First-Order Radio Energy Model [13].

Transmission energy:

$$E_{tx}(k,d) = E_{elec} \cdot k + \epsilon_{amp} \cdot k \cdot d^2 \tag{6}$$

Reception energy:

$$E_{rx}(k) = E_{elec} \cdot k \tag{7}$$

Residual energy after transmission:

$$E_{residual} = E_{previous} - (E_{tx} + E_{rx}) \tag{8}$$

where E_{elec} is 50 nJ/bit, and ϵ_{amp} is 100 pJ/bit/m$^{2.}$

3.5. Algorithm 1: Backward Token-Based Routing Procedure

Input:
Set of sensor nodes N, sink node S, initial node energy E_0, packet size k
Output:
Loop-free routing tree with token-controlled collision-free data transmission

Step 1: Network Initialization

1. Deploy N sensor nodes randomly in the sensing area
2. Assign initial energy $E_0 = 1$Joules to each node
3. Initialize the hop count of the sink node:
   $HopCount_S = 0$
4. Initialize routing tables as empty

Step 2: Backward Token Generation at Sink Node

5. Sink node generates a backward token BT
6. Token structure:
   BT = {TokenID, SourceID, ParentID, HopCount, ResidualEnergy, SequenceNumber}
7. Broadcast token to neighboring nodes

Step 3: Token Propagation and Hop Count Update

8. For each node N_i receiving token from node N_j:
   HopCount_i = HopCount_j + 1

```
    9.  If received hop count is smaller than stored hop count:
                Update HopCount_i
                Accept token
        Else:
                Discard token

Step 4: Path Cost Computation
    10. Compute routing path cost:
                $PathCost_i = PathCost_j + \alpha d_{ij} + \beta \frac{1}{E_j}$
                where $d_{ij}$= Euclidean distance, $\alpha = 0.6$, and $\beta = 0.4$

Step 5: Parent Node Selection
    11. Select parent node using weighted decision function:
                $Parent_i = \arg\min\left(0.5 \cdot HopCount_j + 0.3 \cdot PathCost_j - 0.2 \cdot Energy_j\right)$

    12. Update routing table:
                Store ParentID
                Store HopCount
                Store ResidualEnergy
                Store PathCost

Step 6: Routing Tree Construction
    13. Repeat Steps 8–12 until all nodes receive a backward token
    14. Construct a hierarchical routing tree rooted at the sink node

Step 7: Token-Based Medium Access Control
    15. Leaf node requests transmission permission from the parent node
    16. If token available:
                Grant transmission permission
        Else:
                Wait until the token is received
    17. Only one leaf node transmits data at a time

Step 8: Data Transmission Phase
    18. Leaf node senses environment
    19. Transmit sensed data to parent node
    20. Parent node performs aggregation
    21. Forward aggregated data toward the sink node
    22. Repeat until data reaches sink node

Step 9: Residual Energy Update
    23. Update transmission energy:
                $E_{tx}(k, d) = E_{elec} \cdot k + \epsilon_{amp} \cdot k \cdot d^2$
    24. Update reception energy:
                $E_{rx}(k) = E_{elec} \cdot k$
    25. Update node residual energy:
                $E_{new} = E_{old} - (E_{tx} + E_{rx})$

Step 10: Token Loss Detection and Recovery
    26. If the node does not receive a token within the timeout interval:
                Assume token loss
    27. Sink regenerates a token
    28. Duplicate tokens discarded using sequence number comparison
```

```
Step 11: Periodic Token Regeneration
    29. Sink generates a new backward token every:
            $T = 5$ seconds
    30. Update the routing tree dynamically according to residual energy

Step 12: Loop-Free Routing Guarantee
    31. Ensure routing condition:
            $HopCount_{child} > HopCount_{parent}$
```

3.6. Loop-Free Routing Guarantee

The routing structure remains loop-free because parent selection satisfies:

$$HopCount_i > HopCount_{parent(i)} \tag{9}$$

Since hop count strictly decreases toward the sink node, cyclic routing paths cannot exist within the constructed topology [14].

3.7. Token-Controlled Data Transmission Phase and Complexity

After topology formation, the backward token regulates channel access across the network. Only nodes holding a valid token are allowed to transmit data. This provides:

- collision avoidance
- controlled medium access
- reduced retransmissions
- improved channel utilization

Leaf nodes transmit sensed data to parent nodes using the minimum-cost routing path identified during token propagation. Intermediate nodes aggregate received data and forward it toward the sink node. Token loss is detected using timeout monitoring and sequence number verification.

If a node fails to receive the token within a predefined interval:

1. Token loss is assumed
2. Sink node regenerates token
3. Duplicate tokens are discarded using sequence IDs

This ensures continuous routing availability and prevents network deadlock conditions. The complexity of routing tree construction depends on token propagation across all nodes: $O(N)$ where N represents the total number of sensor nodes. Since each node processes the token once per iteration, the algorithm remains scalable for medium-sized WSN deployments. The flow diagram in Fig. 1 illustrates the proposed method in detail.

4 SIMULATION SETUP AND PERFORMANCE EVALUATION METHODOLOGY

To evaluate the effectiveness of the proposed Backward Token-Based Routing Framework (BTBRF), simulation experiments were conducted using the QualNet discrete-event network simulator. The simulation environment was designed to analyze the performance of the proposed routing framework under varying network sizes and traffic conditions using standard wireless sensor network modeling assumptions. The performance of the proposed method was compared with conventional token-based communication mechanisms using throughput, packet delivery ratio, end-to-end delay, and energy consumption as evaluation metrics.

4.1. Network Deployment Model

A static wireless sensor network consisting of randomly distributed sensor nodes was considered in the simulation environment. The sensor nodes were deployed uniformly within a square sensing region of size $500 \times 500\text{m}^2$. The number of sensor nodes was varied from 20 to 100 to evaluate the scalability performance of the proposed routing framework under different network densities. All sensor nodes were assumed to be stationary after deployment and equipped with identical initial energy levels. The sink node was placed at the center of the sensing area and assumed to have unlimited energy and computational capability. A hierarchical routing tree structure was constructed using sink-initiated backward token propagation prior to the data transmission phase.

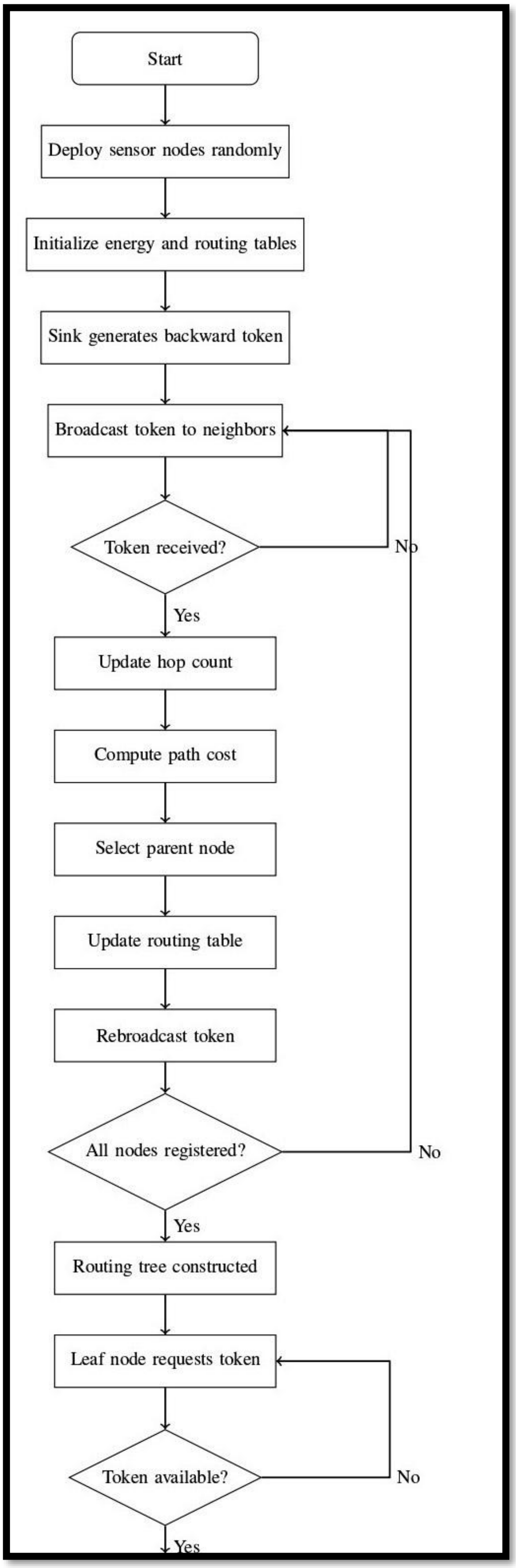

Fig. 1. Flow diagram of the proposed method

4.2. Radio Propagation and MAC Layer Model

The wireless communication channel was modeled using the Two-Ray Ground propagation model [15], which provides a realistic representation of signal attenuation in medium-scale outdoor wireless sensor network environments. Sensor nodes communicated using the IEEE 802.15.4 MAC protocol [16], which is widely adopted for low-power wireless sensor network applications due to its energy efficiency and low data-rate characteristics. The operating frequency of the communication channel was set to 2.4 GHz, and the transmission data rate was configured as 250 kbps, consistent with the IEEE 802.15.4 standard.

4.3. Energy Consumption Model and Traffic Model

The simulation adopted the widely used First-Order Radio Energy Model [13] to estimate transmission and reception energy consumption of sensor nodes. The energy required for transmitting a k-bit packet over distance $d$was calculated as:

$$E_{tx}(k,d) = E_{elec} \cdot k + \epsilon_{amp} \cdot k \cdot d^2 \tag{10}$$

Similarly, the energy required for receiving a k-bit packet was computed as:

$$E_{rx}(k) = E_{elec} \cdot k \tag{11}$$

where:

- E_{elec} = 50nJ/bit represents the electronics energy consumption
- ϵ_{amp} = 100pJ/bit/m^2 represents the transmit amplifier energy

Each sensor node was initialized with 1 Joule of energy at the beginning of the simulation. Residual energy values were updated dynamically during routing operations based on transmission and reception activities. A Constant Bit Rate (CBR) traffic model was used to generate sensing data from sensor nodes toward the sink node. Each sensor node generated fixed-size data packets of 128 bytes at a transmission rate of 2 packets per second. The packet transmission interval between consecutive packets was configured as 0.5 seconds. Data packets generated by leaf nodes were forwarded toward the sink node through intermediate parent nodes based on the routing tree constructed using backward token propagation.

4.4. Backward Token Configuration

In the proposed routing framework, the sink node periodically generates backward tokens to construct and maintain the hierarchical routing tree structure. The backward token contained routing information fields, including:

- token identifier
- source node identifier
- parent node identifier
- hop count
- residual energy
- sequence number

The token size was configured as 24 bytes, and tokens were propagated through multicast dissemination across the network topology. Backward tokens were regenerated periodically at an interval of 5 seconds to update routing paths dynamically according to residual node energy variations. Token loss detection was implemented using a timeout monitoring mechanism combined with sequence number verification. When a token loss was detected, the sink node regenerated a new token to maintain continuous routing availability.

4.5. Routing Tree Construction Mechanism and Simulation Parameters

The hierarchical routing tree was constructed using sink-initiated backward token propagation. Each node receiving the backward token computed its hop count, evaluated path cost, and selected an optimal parent node based on a weighted decision function incorporating hop distance, residual energy, and communication cost. Routing decisions were updated dynamically during periodic backward token regeneration to ensure balanced energy utilization across the network. The monotonic decrease of hop count values toward the sink node ensured loop-free routing topology formation. Table 2 summarizes the simulation parameters used in the experimental setup.

Table 2. Simulation Parameters

Parameter	Value
Simulation tool	QualNet
Network area	500 × 500 m²
Number of nodes	20–100
Node deployment	Random uniform
Sink position	Center
Node mobility	Static
Simulation time	600 s
Initial node energy	1 Joule
Packet size	128 bytes
Traffic type	CBR
Packet generation rate	2 packets/sec
Transmission interval	0.5 s
Token size	24 bytes
Token interval	5 s
Propagation model	Two-Ray Ground
MAC protocol	IEEE 802.15.4
Channel frequency	2.4 GHz
Data rate	250 kbps
Energy model	First-order radio model
Number of simulation runs	25
Confidence interval	95%

4.6. Performance Evaluation Metrics

The performance of the proposed backward token-based routing framework was evaluated using the following metrics.

Packet Delivery Ratio (PDR)

Packet Delivery Ratio quantifies the fraction of transmitted packets that successfully arrive at the sink node and reflects the reliability of multi-hop forwarding under the constructed routing topology.

$$PDR = \frac{\text{Packets received}}{\text{Packets sent}} \tag{12}$$

Throughput

Throughput represents the total amount of successfully received data at the sink node per unit simulation time.

$$Throughput = \frac{\text{Total received data (bits)}}{\text{Simulation time}} \tag{13}$$

End-to-End Delay

End-to-end delay represents the average time required for a data packet to travel from the source node to the sink node.

$$Delay = \frac{\sum(t_{receive} - t_{send})}{N} \tag{14}$$

Energy Consumption

Energy consumption represents the total energy utilized by sensor nodes during communication.

$$E_{total} = \sum_{i=1}^{N} (E_{initial,i} - E_{final,i}) \tag{15}$$

5 RESULTS AND DISCUSSION

This section presents the performance evaluation of the proposed BTBRF and compares its behavior with the conventional single-token communication approach under varying network sizes ranging from 20 to 100 sensor nodes. The evaluation was performed using QualNet simulation [17] based on throughput, packet delivery ratio (PDR), end-to-end delay, and energy consumption metrics. Each simulation scenario was executed over 25 independent runs, and the reported results correspond to the average values obtained with a 95% confidence interval to ensure statistical reliability.

Fig. 2 illustrates the variation of packet delivery ratio with respect to the increasing number of sensor nodes for both the single-token and backward token communication mechanisms. The results show that the proposed backward token routing framework consistently achieves a higher packet delivery ratio compared with the conventional single-token approach for network sizes between 20 and 80 nodes. This improvement is mainly due to controlled channel access enabled by token-authorized transmission scheduling, which reduces packet collisions and retransmissions. Similar behavior has been observed in earlier token-scheduled wireless communication systems where controlled channel access reduced retransmission probability under moderate network load conditions [5]. Table 3 presents the improvement of the packet delivery ratio with the proposed method.

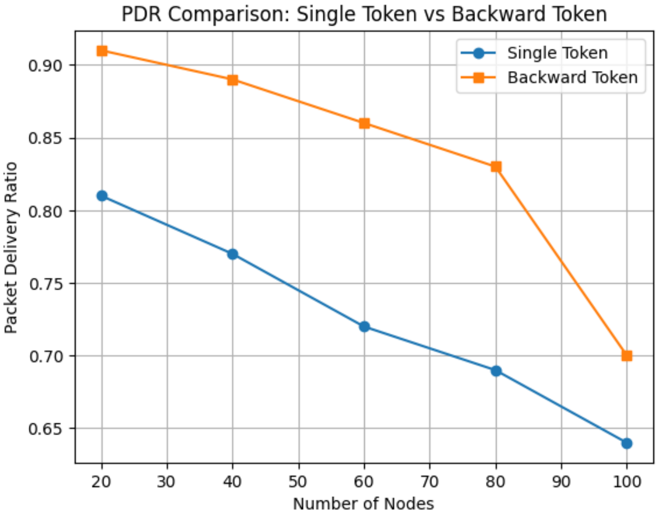

Fig. 2. Packet Delivery Ratio

Table 3. Performance analysis in terms of Packet Delivery Ratio

Nodes	Single Token	Backward Token	Improvement
20	0.81	0.91	+12.3%
40	0.77	0.89	+15.6%
60	0.72	0.86	+19.4%
80	0.69	0.83	+20.3%

As the number of nodes increases beyond 80, the packet delivery ratio of both approaches decreases due to increased contention and routing overhead. However, the backward token mechanism maintains improved reliability across most evaluated network sizes. The observed improvement confirms that sink-initiated backward token propagation enables more efficient coordination of node transmissions in dense wireless sensor network deployments. Fig. 3 compares the total energy consumption of the proposed backward token routing framework with the conventional single-token mechanism. The backward token mechanism consistently consumes less energy compared with the single-token approach due to reduced retransmissions and improved routing coordination. Table 4 presents the reduction in energy consumption with the proposed method.

Fig. 4 presents the variation of end-to-end delay for both routing mechanisms as the number of sensor nodes increases. The proposed backward token routing framework achieves lower delay compared with the single-token mechanism across all evaluated scenarios. Table 5 presents the reduction in end-to-end delay with the proposed method. The reduction in delays is mainly attributed to controlled token-based transmission scheduling, which reduces channel contention and buffering delays at intermediate routing nodes. Fig. 5 illustrates the throughput performance comparison between the single-token and backward token routing mechanisms under different network sizes. The backward token routing framework consistently maintains higher throughput across all evaluated scenarios. Table 6 presents the improvement of throughput with the proposed method. The consistent throughput advantage observed across all evaluated node densities indicates that backward-token scheduling limits simultaneous medium contention events during upstream forwarding.

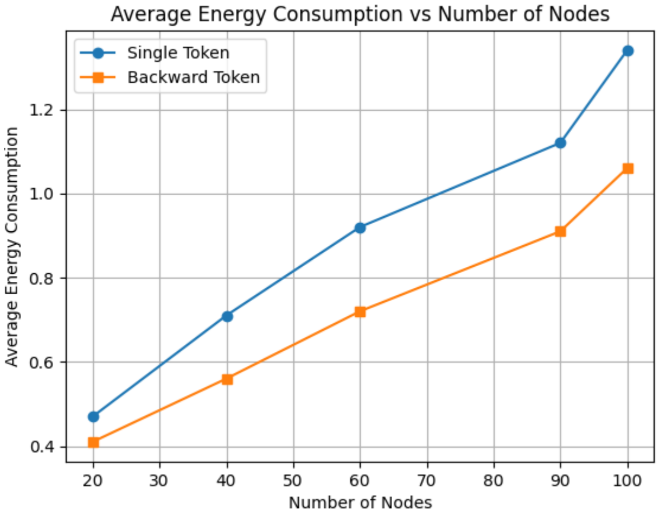

Fig. 3. Average Energy Consumption

Table 4. Performance analysis in terms of Energy Consumption

Nodes	Single Token	Backward Token	Energy Reduction
20	0.45	0.40	11.1%
40	0.70	0.55	21.4%
60	0.92	0.72	21.7%
80	1.12	0.90	19.6%
100	1.35	1.05	22.2%

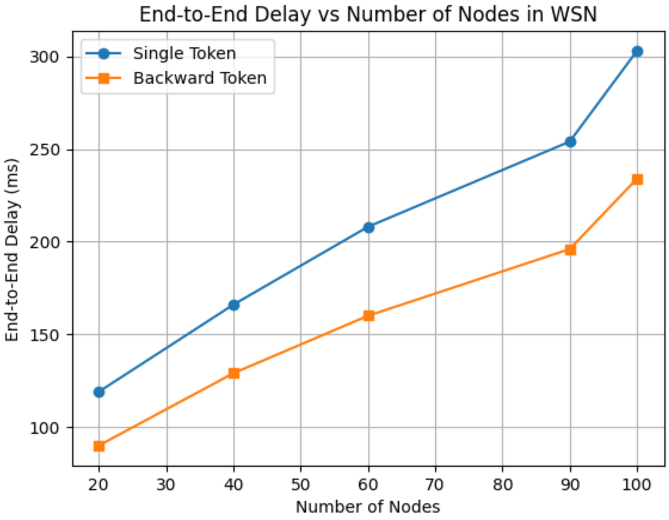

Fig. 4. End-to-end delay

Table 5. Performance analysis in terms of End-to-end delay

Nodes	Single Token	Backward Token	Delay Reduction
20	120 ms	90 ms	25.0%
40	165 ms	90 ms	45.4%
60	210 ms	160 ms	23.8%
80	255 ms	195 ms	23.5%
100	305 ms	235 ms	22.9%

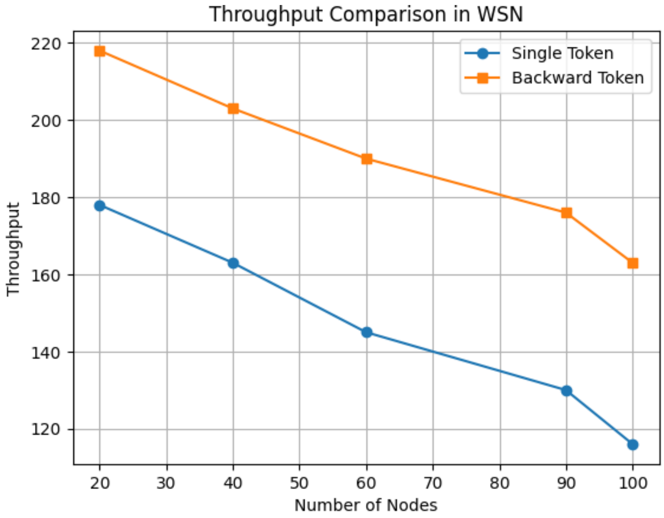

Fig. 5. Throughput

Table 6. Performance analysis in terms of Throughput

Nodes	Single Token	Backward Token	Improvement
20	178	218	22.4%
40	163	202	23.9%
60	145	190	31.0%
80	130	178	36.9%
100	115	163	41.7%

5.5. Discussion

The primary advantage of the proposed backward token routing framework lies in its ability to regulate node participation during communication using sink-generated tokens. Unlike contention-based approaches, where multiple nodes compete simultaneously for channel access, the backward token mechanism ensures that only authorized nodes transmit data at a given time.

This controlled transmission scheduling reduces:

- packet collisions
- retransmission overhead
- idle listening energy consumption
- buffer congestion at intermediate nodes

As a result, the routing tree constructed using backward token propagation improves overall network reliability and communication efficiency. The current evaluation assumes static node placement and periodic traffic generation; performance under bursty sensing conditions will be investigated in future work.

6 CONCLUSION

The proposed backward token-based routing framework enables hierarchical routing-tree construction through sink-initiated token propagation and supports controlled transmission scheduling in multi-hop wireless sensor networks. Parent selection based on hop distance, path cost, and residual energy allows balanced routing decisions while maintaining a loop-free topology using monotonic hop-count constraints. Regulating channel access through token authorization reduces contention among transmitting nodes and improves coordination during upstream data forwarding. Simulation results obtained using the QualNet platform for networks containing 20 to 100 sensor nodes indicate consistent improvements in packet delivery ratio and throughput, together with reduced end-to-end delay and lower overall energy consumption compared with the conventional single-token communication approach. Periodic regeneration of backward tokens also supports adaptive routing updates as node energy decreases during operation. These observations suggest that backward token-assisted routing can provide a practical mechanism for improving communication stability in medium-scale static wireless sensor deployments. Future investigations will examine performance under larger network sizes, non-uniform traffic conditions, and scenarios involving mobile sink nodes.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ETHICS STATEMENT

This study did not involve human or animal participants and therefore did not require ethical approval.

STATEMENT OF CONFLICT OF INTERESTS

The authors declare no conflicts of interest related to this study.

LICENSING

REFERENCES

[1] B. Suresh and G. S. C. Prasad, "An energy efficient secure routing scheme using LEACH protocol in WSN for IoT networks," *Measurement Sensors*, vol. 30, p. 100883, Aug. 2023, doi: 10.1016/j.measen.2023.100883.

[2] Z. Aliouat and M. Aliouat, "Efficient management of energy budget for PEGASIS routing protocol," in *Proc. 6th Int. Conf. Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, Sousse, Tunisia, 2012, pp. 516–521, doi: 10.1109/SETIT.2012.6481966.

[3] Y.-P. Kim, E. Jung, and Y.-J. Park, "A radio-aware routing algorithm for reliable directed diffusion in lossy wireless sensor networks," *Sensors*, vol. 9, no. 10, pp. 8047–8072, Oct. 2009, doi: 10.3390/s91008047.

[4] J. Huang, Y. Li, and H. Yu, "Design and implementation of multi-hops wireless sensor network routing protocol based on HEED," in *Proc. IEEE 17th Int. Conf. Communication Technology (ICCT)*, Chengdu, China, 2017, pp. 598–601, doi: 10.1109/ICCT.2017.8359706.

[5] P. Wang and W. Zhuang, "A token-based scheduling scheme for WLANs supporting voice/data traffic and its performance analysis," *IEEE Transactions on Wireless Communications*, vol. 7, no. 5, pp. 1708–1718, May 2008, doi: 10.1109/TWC.2007.060889.

[6] T. Narasimhan and S. S. Deepa, "QoS-Ring: A token ring approach for QoS provisioning in ad-hoc networks," in *Proc. 4th Int. Conf. Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, India, 2013, pp. 1–5, doi: 10.1109/ICCCNT.2013.6726830.

[7] O. Mirabella, M. Brischetto, A. Raucea, F. Bannò, and V. Di Martino, "WTB: A token-based wireless communication over 802.11b," in *Proc. IEEE Int. Symp. Industrial Electronics (ISIE)*, Bari, Italy, 2010, pp. 3505–3512, doi: 10.1109/ISIE.2010.5637482.

[8] I. Nakajima, K. E. Mitsuhashi, H. Juzoji, K. Ozaki, N. Nakamura, and Y. Odaya, "The use of a wireless token ring protocol to monitor vital data in mute swans," in *Proc. 23rd Int. Symp. Wireless Personal Multimedia Communications (WPMC)*, Okayama, Japan, 2020, pp. 1–6, doi: 10.1109/WPMC50192.2020.9309466.

[9] Z. A. Abduljabbar *et al.*, "Session-dependent token-based payload enciphering scheme for integrity enhancements in wireless networks," *Journal of Sensor and Actuator Networks*, vol. 11, no. 3, p. 55, Sep. 2022, doi: 10.3390/jsan11030055.

[10] H. Cui, X. Yang, W. Yang, B. Qin, and X. Yi, "Token-based biometric enhanced key derivation for authentication over wireless networks," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 4, pp. 2347–2357, Jul.–Aug. 2023, doi: 10.1109/TNSE.2023.3246439.

[11] J. Hillyard and J. L. Taylor, "Token passing data transfer mechanism for reservation-based protocols," U.S. Patent US20090080456A1, Mar. 26, 2009. Available: https://patents.google.com/patent/US20090080456A1

[12] F. Guangyu and C. Dongxiang, "Method for passing token in wireless dynamic token ring network," China Patent CN101998659B, Mar. 30, 2011. Available: https://patents.google.com/patent/CN101998659B

[13] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Maui, HI, USA, 2000, pp. 10 pp. vol.2-, doi: 10.1109/HICSS.2000.926982.

[14] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking,* 2000, pp. 56-67, doi: 10.1145/345910.345920.

[15] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2002.

[16] IEEE Standard for Low-Rate Wireless Networks, in *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691.

[17] Scalable Network Technologies, *QualNet Network Simulator Documentation*, Version 7.4, Los Angeles, CA, USA, 2020.