RERESDA: AN ENERGY-EFFICIENT REDUNDANCY ELIMINATION AND SECURE DATA AGGREGATION FRAMEWORK FOR WIRELESS SENSOR NETWORKS

Sunil S harakannanavar[1], Sumathi M S[2], Srinivasan P[3], Sapnakumari C[4] and Rangaswamy Y[5]

[1]Department of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology (NMIT), Nitte (Deemed to be University), Nitte University Capus, Yelahanka, Bangalore, Karnataka, India
[2]Department of Electronics & Telecommunication Engineering, BMS Institute of Technology and Management, Bengaluru, Karnataka, 560064, India.
[3]Department of Electronics & Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Nagercoil Campus.
[4]Department of Electronics and Communication Engineering, Sapthagiri NPS University, Bangalore, Karnataka, India.
[5]Department of Electronics and Communication Engineering, Dr. Ambedkar institute of Technology Bengaluru, Karnataka, 560056, India.

ABSTRACT

Wireless Sensor Networks (WSNs) are being used more for monitoring and surveillance, where nodes with limited energy resources must send a lot of sensed data. One big problem with these kinds of networks is that nodes run out of power quickly because they send the same data repeatedly. This has a direct impact on the network's lifetime and reliability. Many data aggregation methods have been suggested to cut down on communication overhead, but most of them only deal with redundancy between nearby nodes and does not do a good job of stopping repeated transmissions from the same node over multiple sensing rounds. Also, security concerns are often not fully considered in redundancy elimination systems. This paper introduces a Robust and Efficient Redundancy Elimination Secure Data Aggregation (RERESDA) model for clustered Wireless Sensor Networks (WSNs) to address these limitations. The suggested method presents a pattern-based data representation system that takes advantage of changes in sensed data over time. Sensor nodes only send data to the cluster head when they notice a change in the pattern they are making. This keeps them from sending data that is not needed. Also, when a cluster has similar data patterns, the cluster head picks a representative node based on how much energy is left in it. This keeps data safe while making sure that energy use is balanced. We use MATLAB-based simulations to test how well the proposed scheme works with a network of 40 sensor nodes spread out over a 100 m × 100 m area. Experimental results indicate that the proposed model diminishes overall energy consumption by as much as 56% in comparison to non-aggregation methods, while concurrently reducing bandwidth utilization. The results show that RERESDA really does improve energy efficiency and network lifetime by getting rid of redundancy and safely aggregating data at the same time.

KEYWORDS

Wireless Sensor Networks, Secure Data Aggregation, Redundancy Elimination, Energy Efficiency, Clustering Techniques.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are key parts of many modern systems where data is sampled, such as in smart farming, health care, smart cities, environment scanning, in industry, and militarily people “keeping an eye” on places. In such systems, many sensor nodes can be spread in a wide area for the purpose of capturing important information such as temperature, humidity, pressure, vibration, motion, etc., with constant updates which they can then send back to a base station [1]. The base station then analyses the observations for judging or control. Even though WSNs have many options of use, they are restricted by low battery life, very low processing power, and very limited communication resources. Communication consumes the greatest percentage of energy among all operations of a node, giving high priority to minimize or remove redundancy when designing the network. When dense clusters of sensors are in a geographical area, they will often observe the same environmental factors, and transmit redundant, repetitious data. If this redundancy is not handled and ruled properly, it will cost in energy waste, quickening sensor death, leading to contention of added sensors, and increasing the ratio of failure. In many cases, advancement on real-time large-scale infrastructure or remote environmental observation, placement of WSNs themselves becomes impractical or simply impossible to replace or recharged nodes batteries [2]. Therefore, to have WSNs working in the long and short terms, cost (redundant transmission) must be reduced while studied data must be kept in safe condition and free of loss. It therefore gives necessity for efficient data aggregation that robustly intelligently eliminates repetitive data, while maximizing the use of energy with no loss of data integrity. In Figure 1, Sensor nodes sense environmental data and send it to Cluster Heads (CHs), which aggregate data and forward it to the Base Station. Communication dominates energy consumption [3].

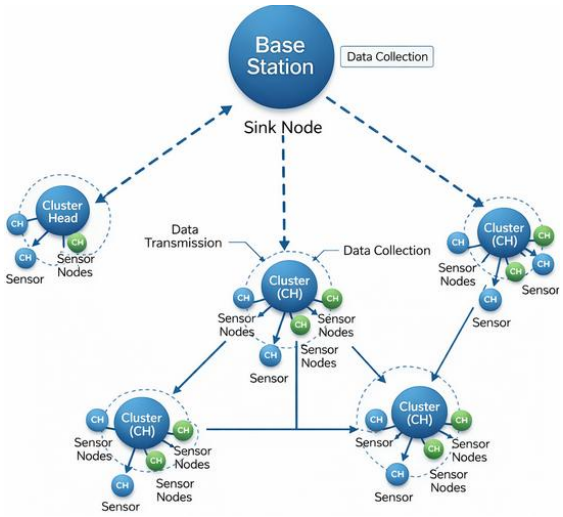

Figure. 1. Cluster-based wireless sensor network architecture for remote monitoring applications.

The main issue this work deals with is that clustered Wireless Sensor Networks use too much energy because sensor nodes send the same data to their cluster heads more than once. Redundancy occurs not only among adjacent nodes detecting analogous conditions (inter-node redundancy) but also within individual nodes across successive sensing rounds when the sensed values remain constant (intra-node redundancy). Most traditional data aggregation methods assume that all nodes send data at regular intervals, even if the data that was sensed has changed a lot [4]. This causes extra communication overhead, more bandwidth use, and early energy loss for both sensor nodes and cluster heads. The aggregation process must also follow strict rules, such as limited node energy, low computational power, static node placement, and the need for

secure data delivery. So, the problem is to come up with a secure way to combine data that gets rid of both inter-node and intra-node redundancy while still being able to run on the limited energy and resources of WSNs.

There are a lot of systems that have been made to save power and cut down on unnecessary data sending in WSNs. Some of these focus on spatial closeness by gathering data from nodes in a cluster that are close to each other. These can only fix half of the problem because they don't get rid of duplicate data that has been sent [5]. Some of these don't completely get rid of the risk of duplicate data because the sensor still sends the same data in one iteration and then sends the same data again in the next. Some schemes also use complicated routing, costly optimization, or machine learning algorithms that don't work well with all of the sensor nodes that have limited power. Several studies have examined security in relation to either data reduction or data relocation. This, along with the delivery method, brings with it goals for recovery, computation, and safety. These systems can't meet all three needs in a simple but scalable way [6]. The primary aims and contributions of this work are encapsulated as follows:

- To suggest a strong and effective Redundancy Elimination Secure Data Aggregation (RERESDA) model for clustered Wireless Sensor Networks.
- To implement a pattern-based data representation system that identifies alterations in sensed data over successive iterations and mitigates unnecessary transmissions.
- To get rid of data redundancy between nodes and within nodes without making sensor nodes do complicated math.
- To add a secure aggregation mechanism that keeps data safe and private while it is being sent.
- To show through simulation that the suggested model uses up to 56% less energy and makes better use of bandwidth than methods that don't use aggregation.

The proposed method is a good and useful way to extend the life of a network while making sure that data aggregation is safe and reliable in WSNs with limited energy. This article is organized as follows. Section 2 summarizes the existing works on data aggregation, removing duplicate data and power-aware communication in Wireless Sensor Networks. Section 3 presents the Robust and Efficient Redundancy Elimination Secure Data Aggregation (RERESDA) scheme that we propose, in which we show how the clusters are formed, how the pattern is created, how duplicate data is eliminated, and how security issues are handled. Section 4 shows the simulation environment, simulation parameters, and the experimental results; it also compares the performance of our scheme to other recent techniques. Finally, Section 5 concludes the paper by presenting the main conclusions and discussing future research directions.

2. LITERATURE SURVEY

This section gives a detailed look at current routing protocols and network architectures. They are divided into three groups: traditional heuristic-based methods, machine learning–assisted methods, and hybrid optimization frameworks. The focus is on how they reduce redundancy, make communication more energy-efficient, adapt routing, and safely collect data in wireless sensor and IoT networks.

Aggarwal et al. [1] created EndRE, a service for enterprise networks that gets rid of end-system redundancy. EndRE, on the other hand, does chunk-level redundancy elimination directly at the end hosts, which means that it can work even when there is encrypted traffic. This is different from traditional middlebox-based solutions. Sample Byte fingerprinting cuts down on the amount of processing power needed while still being able to find duplicates. Testing on real enterprise

traffic traces showed that bandwidth savings were about 25–30%, latency was lower, and processing throughput was high. Lu et al. [2] suggested a frequency-based chunking (FBC) method to make data deduplication work better. The method doesn't use traditional content-defined chunking. Instead, it looks for byte patterns that happen often to find the best chunk boundaries. This strategy cuts down on the number of chunks made by a lot while keeping the ratio of duplicate chunks low. Tests showed that FBC cut the number of chunks by up to four times compared to other methods. Saha et al. [3] introduced Combi Header, a protocol-level optimization method designed to reduce the overhead linked to multiple shim headers in systems that eliminate redundancy. The proposed method lowers protocol overhead by combining several headers into one composite structure. This does not change the accuracy of redundancy detection. The simulation results showed that the system was more efficient and had less overhead.

Salah ud Din et al. [4] talked about the problem of sending the same data over and over in heterogeneous wireless multimedia Internet of Things (IoT) networks. Their method takes advantage of the correlation between multimedia data streams to stop unnecessary transmissions. The performance test showed that the device used less energy, lasted longer, and had a higher throughput. Aswale and Ghorpade [5] put forward a geographic multipath routing protocol for wireless multimedia sensor networks (WMSNs). The protocol uses a triangle-based link quality metric to reduce interference between paths. The simulation results showed that the new routing schemes had higher packet delivery rates, shorter end-to-end delays, and better energy efficiency than the old ones. Lobiyal and Abawajy [6] created a multipath routing algorithm for WMSNs that saves energy by spreading traffic across several paths that are aware of energy use. This stops nodes from running out of power too soon. The simulation showed that the network's lifetime and throughput got a lot better when there was a lot of multimedia traffic. Raja and Mangai [7] came up with a load-balancing routing scheme for delivering multimedia data over wireless mesh networks that is based on the firefly algorithm. The bio-inspired optimization mechanism spreads out network load in a way that uses the least amount of energy, which leads to less delay and better overall energy efficiency. Awad [8] suggested a better way to place relay nodes for multisource multipath routing in WMSNs using a Gaussian distribution model. This method improves network connectivity and energy efficiency, resulting in higher packet delivery rates and less routing overhead.

Habib and Moh [9] put forward a strong routing protocol for WMSNs that is based on evolutionary games. Routing decisions change based on the strategies of the nodes and the amount of energy they have left. The results of the simulation showed that the network was more stable, had less packet loss, and lasted longer. Tripathi et al. [10] suggested a load-aware multipath data forwarding scheme to make wireless sensor networks last longer. The scheme cuts down on congestion and balances energy use across the network by sending traffic based on node load and remaining energy. Xu et al. [11] came up with an energy-efficient region-based source routing protocol that aims to make the network last as long as possible. The protocol puts nodes into regions to improve routing paths, which leads to better energy balance and longer network operation. Govindaraj and Deepa [12] utilized a capsule neural network-based learning model for energy optimization in IoT-enabled wireless sensor networks. The suggested model worked better for routing and saved more energy than traditional neural network methods. Ambareesh and Madheswari [13] put forward HRDSS-WMSN, a multi-objective optimal routing protocol for WMSNs that combines the Red Deer Swarm Algorithm with SALP swarm optimization. The protocol improves the network's lifetime, end-to-end delay, packet delivery ratio, and energy use all at the same time. The simulation results showed that the system worked better because it used less energy, sent more packets, had less delay, and lasted longer. Gutub [14] put forward a counting-based secret sharing scheme for safe image watermarking. The method makes things more real and secret while keeping the math simple. Experimental validation substantiated enhanced watermark resilience and security. Chen [15] developed an enhanced radial basis

function (RBF) neural network for predicting internet security situation awareness. The improved model was better at making predictions than regular RBF networks. Gope et al. [16] suggested a simple and privacy-protecting way for RFID to authenticate devices in distributed IoT networks. The protocol guarantees secure localization services with minimal computational and communication overhead, rendering it appropriate for smart city applications.

Wani and Khaliq [17] created an intrusion detection system for IoT environments that uses deep learning classifiers and is based on SDN. The centralized SDN architecture made it easier to find attacks and cut down on false alarms. Das and Namasudra [18] proposed a lightweight anonymous mutual authentication framework for big medical data in distributed smart healthcare systems. The protocol protects users' privacy, keeps their data safe, and is resistant to common security attacks with little extra work. Verma et al. [19] looked at the shift cipher technique again to make data security better. The enhanced technique exhibited superior encryption characteristics relative to the traditional shift cipher. Sarkar et al. [20] created a fast web service-based Android app that made the service work better and responded more quickly. Kumar et al. [21] put forward a secure data aggregation scheme for clustered wireless sensor networks that save energy. The method cuts down on unnecessary transmissions while keeping data private, which saves a lot of energy.

Zhang et al. [22] proposed a redundancy-aware data aggregation method utilizing temporal correlation among sensor readings. The method effectively cuts down on communication overhead and makes the network last longer. Elhoseny et al. [23] put forward a lightweight secure aggregation scheme for wireless sensor networks that don't have a lot of power. The protocol keeps strong security guarantees while cutting down on cryptographic overhead. Verma and Mittal [24] put forth a scheme for clustering and data suppression that takes energy into account for large-scale wireless sensor networks. This scheme cut down on unnecessary transmissions and made the network last longer. Chen et al. [25] put forward a framework for IoT-enabled sensor networks that combines redundancy elimination with secure data transmission. This framework reduces communication overhead while keeping data safe. Nguyen et al. [26] proposed an energy-aware temporal data suppression scheme for long-lived wireless sensor networks, successfully mitigating redundant data transmissions and prolonging network longevity. Rani et al. [27] put forward a secure and lightweight data aggregation protocol for wireless sensor networks with limited power, showing that it uses less energy and has less communication overhead. Alsharif et al. [28] introduced a redundancy-aware clustering and aggregation framework for extensive wireless sensor networks, enhancing scalability, minimizing redundancy, and improving energy efficiency. Singh and Namasudra [29] put forward a lightweight authentication and secure data aggregation scheme for IoT-enabled sensor networks that provide strong security with little extra energy use. Zhou et al. [30] proposed a unified energy optimization and redundancy removal framework for clustered wireless sensor networks. The simulation results showed that the network used less energy, sent fewer unnecessary messages, and lasted longer. Darshan and Prashanth [31] proposed EECRPSID, an energy-efficient cluster-based routing protocol for WSN-assisted IoT environments to improve network lifetime. The method integrates secure intrusion detection along with cluster routing to enhance reliability against malicious activity. Their results show that clustering-based optimized routing can reduce energy consumption and improve overall network performance compared to traditional routing techniques. Kashyap et al. [32] presented a fuzzy-based clustering scheme for WSNs focusing on multiple mobile agent itinerary planning to support efficient data collection. The approach improves cluster head selection and load balancing, reducing unnecessary transmissions and energy drain. Experimental outcomes indicate that fuzzy clustering enhances network stability, scalability, and energy efficiency in sensor network deployments.

From the analysis above, current methods do not securely and efficiently deal with both inter-node and intra-node data redundancy at the same time. Traditional aggregation methods do not consider temporal redundancy, ML/DL-based methods add too much computational overhead, and hybrid methods don't have lightweight or unified ways to get rid of redundancy. These limitations drive the development of the Robust and Efficient Redundancy Elimination Secure Data Aggregation (RERESDA) approach, which seeks to minimize redundant transmissions during successive sensing iterations while ensuring low complexity and secure data aggregation in Wireless Sensor Networks.

3. PROPOSED METHODOLOGY

This section presents the proposed methodology for energy-efficient and redundancy-aware data aggregation in Wireless Sensor Networks (WSNs). The framework combines hierarchical clustering, pattern-code–based redundancy suppression, and energy-aware data forwarding to minimize unnecessary transmissions and prolong network lifetime.

3.1. System Overview

The network initially deploys a set of sensor nodes randomly over the sensing area. These nodes are responsible for sensing environmental data and transmitting it to the base station through a hierarchical communication structure. To improve scalability and control communication overhead, the network is logically divided into multiple levels, with each level containing a predefined number of sensor nodes. Each sensor node broadcasts a neighbour discovery message within its communication range. Based on received messages, nodes identify their neighbouring nodes and determine their respective levels in the network hierarchy. This process enables localized communication and efficient cluster formation. Following neighbour discovery, Cluster Head (CH) selection is performed within each cluster. The node with the highest residual energy is selected as the Cluster Head to balance energy consumption across the network. Once elected, each CH broadcasts a notification message to inform cluster members of its role.

After cluster formation, a pattern-code–based data aggregation mechanism is employed. Instead of transmitting raw sensor readings at every sensing round, sensor nodes convert their sensed data into compact pattern codes using a lookup table generated by the CH. Only significant changes in sensed data patterns trigger transmission, thereby eliminating redundant communication.

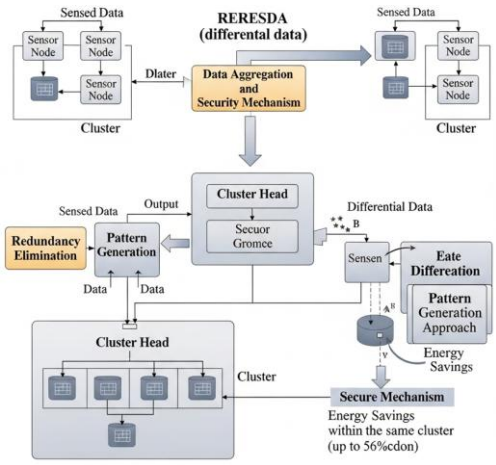

Fig. 2. Architecture and operational flow of the proposed RERESDA

The proposed RERESDA (Redundancy Elimination and Secure Differential Data Aggregation) is a framework designed for clustered wireless sensor networks (WSNs) and IoT applications, focusing on minimizing redundant transmissions, enhancing energy efficiency, and ensuring secure data aggregation. The framework offers several key innovations that improve both efficiency and security in clustered sensor networks. It uses differential redundancy-aware aggregation, meaning that only significant changes in sensor readings are transmitted, which reduces the amount of data sent and saves energy. At the cluster level, pattern-based redundancy elimination identifies dominant trends among sensor readings and forwards only representative information, effectively removing redundant data. Energy-efficient security is achieved by performing encryption after redundant data has been eliminated, which lowers computational effort while ensuring data confidentiality and integrity.

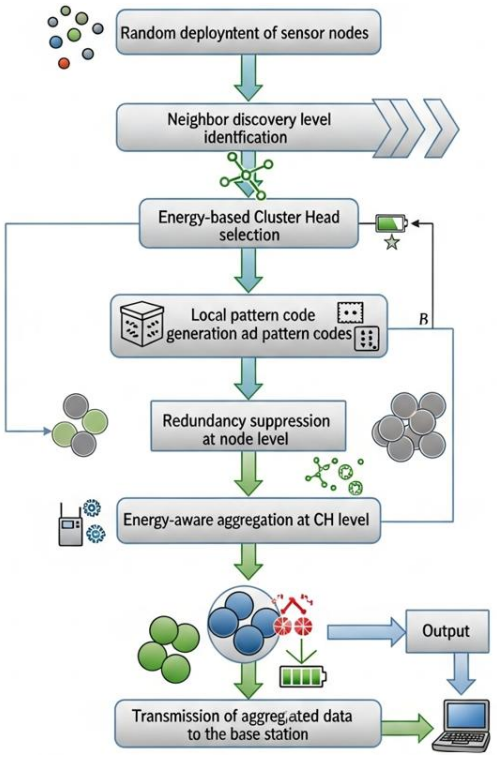

Fig. 3. Workflow of the proposed RERESDA scheme

In addition, the system provides cluster-level intelligence without heavy computation, achieving effective aggregation comparable to machine-learning methods but without the high processing demands. These features lead to substantial practical benefits: overhead communication is reduced because fewer messages are transmitted, cryptographic costs are minimized since only aggregated data is encrypted, and network lifetime is extended due to lower energy consumption. Furthermore, the framework is scalable, efficiently supporting dense sensor deployments without causing excessive data traffic, making it suitable for both small- and large-scale wireless sensors and IoT networks. Finally, RERESDA provides an integrated solution for energy-efficient, secure, and redundancy-aware data aggregation in wireless sensor and IoT networks. Its combined approach of differential encoding, redundancy elimination, pattern-based aggregation, and secure transmission makes it particularly suitable for energy-constrained and large-scale sensor networks. In many sensor networks, nodes within a cluster generate highly correlated data over time and space. Transmitting all raw data directly to the base station leads to unnecessary energy consumption, increased network congestion, and reduced network lifetime. RERESDA addresses these challenges through a cluster-level data processing architecture, combining

differential data representation, redundancy elimination, pattern-based aggregation, and secure transmission.

1. Sensor Node Level Processing

Each sensor node in a cluster collects environmental readings represented as given in equation 1.

$$x_i(t), i = 1,2, \dots, N \tag{1}$$

where $x_i(t)$is the measurement from the i^{th} node at time t. Consecutive readings are often similar due to temporal correlation. To reduce unnecessary transmissions, each node calculates the differential value given in equation 2.

$$\Delta x_i(t) = x_i(t) - x_i(t-1) \tag{2}$$

Only differences that exceed a predefined threshold $\delta(|\ \Delta x_i(t)\ | > \delta)$ are forwarded to the cluster head. This method suppresses minor fluctuations and reduces the data volume transmitted from sensor nodes.

2. Redundancy Elimination at Cluster Head

The cluster head receives differential data from all sensor nodes given in equation 3.

$$D = \{\Delta x_1(t), \Delta x_2(t), \dots, \Delta x_N(t)\} \tag{3}$$

To remove redundant information, the cluster head calculates the correlation coefficient between node readings given in equation 4.

$$\rho_{ij} = \frac{\text{Cov}(\Delta x_i, \Delta x_j)}{\sigma_i \sigma_j} \tag{4}$$

If ρ_{ij}exceeds a correlation threshold τ, the readings from nodes $i$and $j$are considered redundant. Only one representative value is retained for transmission, effectively reducing intra-cluster redundancy.

3. Pattern-Based Aggregation

After eliminating redundant data, the cluster head generates a cluster-level aggregate pattern as given in equation 5.

$$P(t) = \frac{1}{K} \sum_{k=1}^{K} \Delta\, x_k(t) \tag{5}$$

where $K$is the number of non-redundant nodes.
To further optimize transmission, only the differential pattern is sent given in equation 6.

$$\Delta P(t) = P(t) - P(t-1) \tag{6}$$

This ensures that only significant updates are transmitted, further reducing communication energy consumption.

4. Secure Transmission

The aggregated differential data is encrypted before transmission to the base station. Unlike traditional approaches that encrypt raw data, applying security after redundancy reduces cryptographic overhead, conserving energy without compromising confidentiality or integrity.
The energy savings can be expressed as given in equation 7.

$$E_{\text{raw}} = N \cdot E_{\text{tx}} \cdot L_{\text{raw}}, E_{\text{proposed}} = K \cdot E_{\text{tx}} \cdot L_{\text{diff}} \tag{7}$$

Since $K \ll N$and $L_{\text{diff}} \ll L_{\text{raw}}$, energy consumption has been reduced by up to **56%**, significantly extending network lifetime.
Overall, the RERESDA model is a complete process for gathering data in wireless sensor and IoT networks in a way that is energy-efficient, safe, and mindful of redundancy. Because it uses differential encoding, redundancy removal, pattern-based aggregation, and secure transmission all at once, it works especially well for large sensor networks with little energy.

4. Results and Discussion

To quantitatively assess the efficacy of the proposed RERESDA algorithm, various essential metrics are established through mathematical formulations. These metrics measure how well the network works, how well it communicates, and how energy-efficient it is. We compare how well the proposed algorithm works with how well a well-known protocol works without data aggregation. The simulation environment is a clustered wireless sensor network with four clusters, each with ten sensor nodes that were placed randomly. One sensor node from each cluster oversees collecting and sending data from all the other nodes in that cluster.

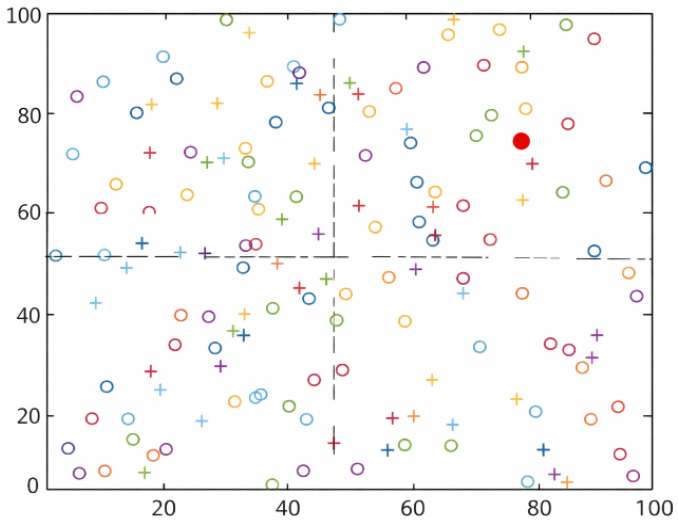

Fig. 4. Random spatial distribution of sensor nodes in the monitoring area with cluster formation and selected cluster head highlighted.

There are 40 sensor nodes randomly spread out across the 100m×100m sensing field, and they stay in one place (not moving) during simulations. The Base Station (BS) is in the middle of the sensing field and is the last place to gather information. We use MATLAB to run all the tests so that we can control them and repeat them. This simulation is used to test the proposed algorithm's energy and bandwidth and to see how it works compared to a protocol that doesn't use aggregation. Figure 4 shows how the network was set up, and table 1 lists the radio and network settings used in the simulation.

Table 1: Network and Radio Configuration Parameters

Parameter	Value
Network area	100 m × 100 m
Number of sensor nodes	40
Number of clusters	4

Nodes per cluster	10
Initial energy	32400 J
$E_{fs}, \varepsilon_{amp}, E_{elect}$	50 nJ/bit, 100 pJ/bit/m², 50 × 10⁻⁹ J
Transmission rate	38.4 kbps
Transmit power (Tx)	52.42 mW
Receive power (Rx)	45.32 mW
Maximum transmission range	60 m
Data rate	100 bits/sec
Bandwidth	10,000 bits/sec
Processing delay	0.1 sec

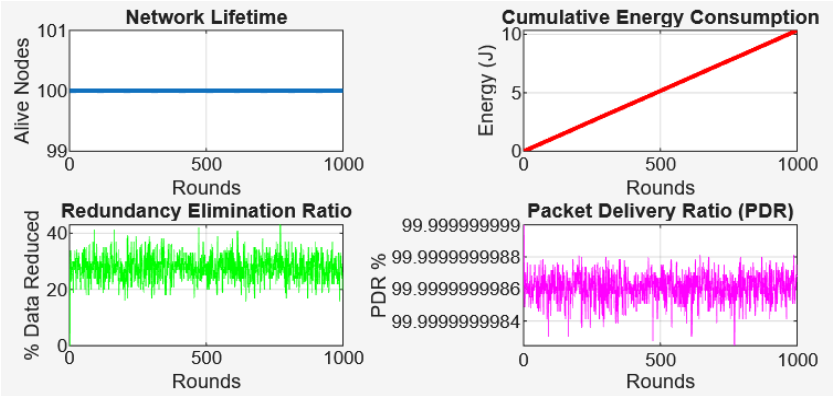

Fig. 5. Performance characteristics of the proposed RERESDA scheme illustrating sustained network lifetime, gradual energy consumption, effective redundancy reduction, and consistently high packet delivery ratio across simulation rounds.

Figure 5(a) shows the number of active sensor nodes over the simulation rounds. It can be observed that all nodes remain alive throughout the entire duration of 1000 rounds. This behaviour indicates that the proposed algorithm effectively reduces energy depletion by limiting unnecessary data transmissions. The stable network operation confirms that the energy-saving mechanisms used in RERESDA are suitable for long-term monitoring applications. The cumulative energy consumption is illustrated in Figure 5(b). The energy usage increases gradually with the number of rounds, indicating controlled energy dissipation across the network. Since only differential and non-redundant data are transmitted, the overall communication cost is significantly reduced. Compared to protocols that transmit raw sensor data, the proposed approach results in lower energy consumption over time. Figure 5(c) presents the redundancy elimination ratio achieved during the simulation. The results show that a considerable amount of redundant data is removed before transmission to the base station. Although small variations occur due to changes in sensor readings, the elimination ratio remains consistently high. This confirms the effectiveness of the cluster-level pattern generation and redundancy elimination process. The packets delivery ratio (PDR) is shown in Figure 5(d). The PDR remains very close to 100% throughout the simulation, indicating reliable data delivery. This demonstrates that reducing data volume through aggregation does not affect communication reliability. The high PDR confirms that the proposed algorithm maintains data integrity while improving energy efficiency.

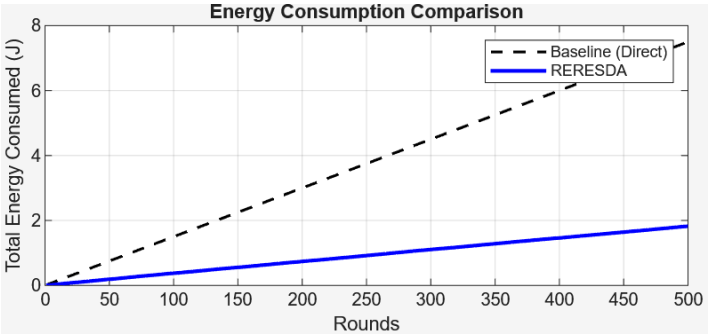

Fig. 6. Comparison of total energy consumption between the baseline direct transmission method and the proposed RERESDA scheme

Figure 6 shows how much energy the baseline direct transmission protocol and the proposed RERESDA algorithm use over several simulation rounds. The baseline shows a quick, almost straight-line rise in energy because raw data is sent repeatedly. RERESDA, on the other hand, uses much less energy because it only sends differential, non-redundant data. After 500 rounds, RERESDA is clearly better than the baseline. This shows how well removing redundancy and aggregating different types of data works.

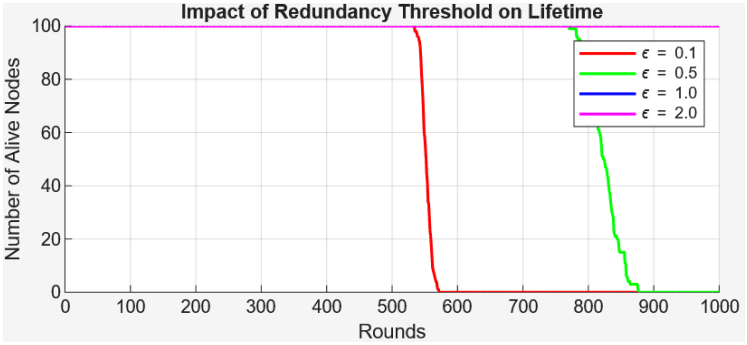

Fig. 7. Effect of redundancy threshold (ε) on network lifetime

Figure 7 illustrates the effect of the redundancy threshold (ϵ) on network longevity. When the thresholds are lower (ϵ=0.1), nodes run out of power faster, and all nodes die after about 560 rounds. As the threshold goes up (ϵ=0.5,1.0,2.0), the network's lifetime gets longer because fewer redundant transmissions use less energy. This shows that changing the redundancy level is an effective way to find a compromise between data accuracy and energy efficiency.

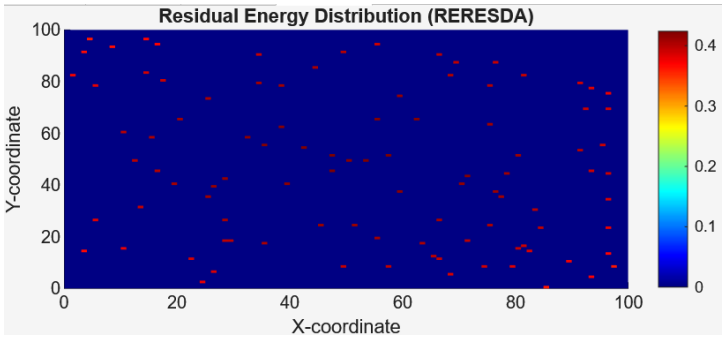

Fig. 8. Spatial distribution of residual energy across sensor nodes

Figure 8 shows how the RERESDA algorithm changes how sensor nodes share the leftover energy. The blue areas show that most of the nodes still have a lot of their original energy. The red spots show that some nodes have less energy left over because they send out different broadcasts at different times. This proves that RERESDA does a good job of spreading out energy use across the network, which makes it last longer.

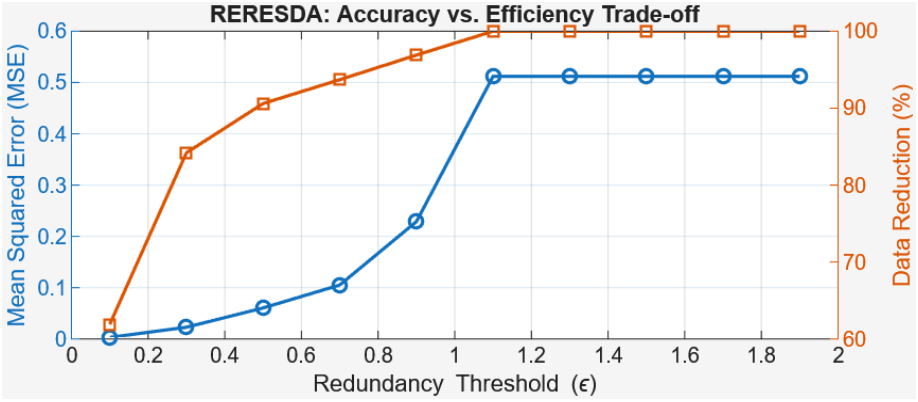

Fig. 9. Accuracy–efficiency trade-off of the proposed RERESDA scheme

Figure 9 shows how the RERESDA algorithm must choose between accuracy and speed. The blue line shows that the Mean Squared Error (MSE) is very low when the redundancy threshold is low, but it goes up quickly after ε ≈ 1 and then levels off. The orange line shows that Data Reduction (%) gets better as the threshold increases, and it gets close to 100% at higher ε values. This shows that RERESDA does a good work of balancing cutting down on unnecessary transmissions while keeping data accuracy at an acceptable level. This lets the network run smoothly without losing a lot of data quality.

The Figure 10 shows speed of end-to-end delay (ms) for our RERESDA scheme as well as the traditional one as the network goes up. RERESDA has a blue line with triangles, and the traditional one has a broken line in red with circles on it. RERESDA goes up but not very quick which tells us that it handles network work well even when the network gets bigger. With the traditional scheme, it does go up but is quick to do this. This shows us that RERESDA takes less time to deliver data as opposed to the traditional way of doing things.

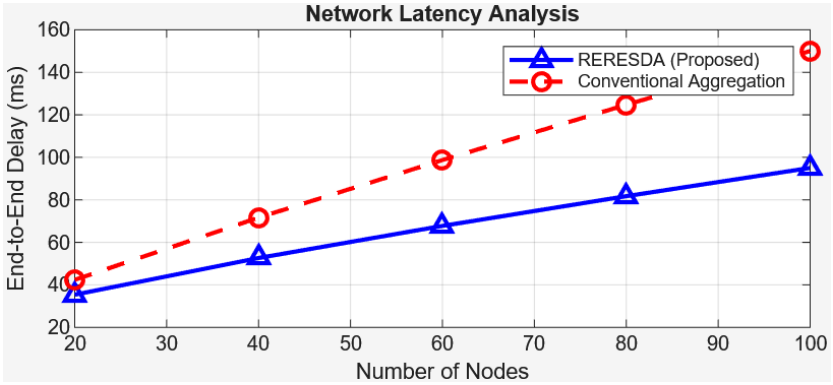

Fig. 10. End-to-end network latency comparison between the proposed RERESDA scheme and the conventional aggregation approach

Figure 11 shows how stable the RERESDA scheme's performance is over 300 rounds of simulation. After a brief period of convergence, the network throughput settles down to a mean value that stays almost the same, with very little variation. This means that there are very few changes during steady operation. The packet delivery ratio stays between 93% and 95% most of the time, with only small changes, even when the randomness is less than 5%. In general, the results show that RERESDA keeps throughput stable and packet delivery reliable, even when the network is acting up randomly.

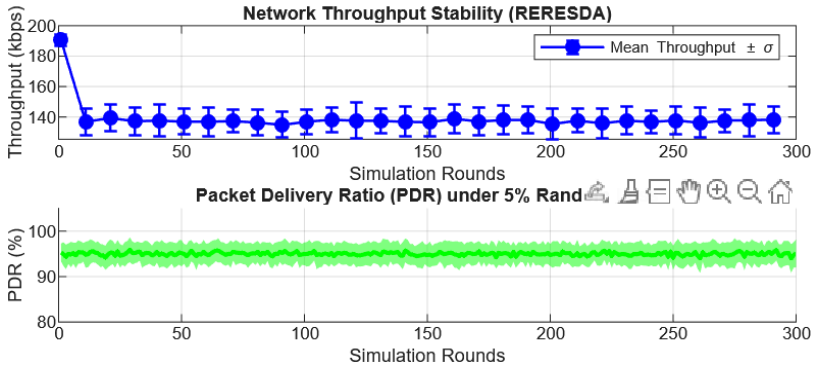

Fig. 11. Performance stability of the proposed RERESDA method over multiple simulation rounds.

Table 2 reveals that the existing approaches mainly resolve one small part only, such as routing improvement, scale adjusting, or a small part of avoiding bug error, without considering safety and collected data increase process together. Although in [4]–[7], they extend life of the network punch or data rate, but they do not treat bug error elimination and safe increase together. This means energy will be used more when we send very many data together. Our designed model RERESDA can treat both bug error elimination and safety increase together in a good way. This made RERESDA save about 56% of energy, but the data is safe and reliable.

Table 2: Comparison of Existing Methods with the Proposed RERESDA Model

Model / Reference	**Primary Objective**	**Key Technique Used**	**Energy Efficiency**	**Redundancy Elimination**	**Security Support**
Salah ud Din et al. [4]	Extending IoT device lifetime	Redundant transmission mitigation in WMIoT	Moderate	Partial	No
Aswale & Ghorpade [5]	Improve network lifetime and throughput	Geographic multipath routing with link-quality metric	Moderate	No	No
Lobiyal & Abawajy [6]	Reduce energy consumption	Energy-efficient multipath routing (EMR)	High	No	No
Raja & Mangai [7]	Optimize multimedia data delivery	Firefly-based load-balanced routing	High	No	No
Proposed RERESDA Model	Energy-efficient, secure, and	Redundancy elimination + secure data	**Very High (≈56% reduction)**	**Yes (Effective)**	**Yes (Built-in security)**

	reliable data aggregation	aggregation			

4. CONCLUSION AND SCOPE OF THE WORK

This study has shown that RERESDA is robust, energy-friendly, eliminates unnecessary data, and keeps data safe for wireless sensors. The model tackles not just data repetition, but also safe data compacting and power saving, which cut down on unnecessary data transfer by quite a lot. The index of performance shows, that RERESDA cuts down on power fuel by 56%, keeps stable data delivery rates, and fast, reliable packet transfer when work takes place in changing network ways. The found evidence bought to saw, that combining data repetition awareness with the security layer, usefully extends the life of the route, and there helps make sure data reaches its destination safely. Using RERESDA for data rich but power weak sensor network grouping and motion sensor workstreams proves particularly fitting.

The proposed RERESDA framework can be improved through the inclusion of an adaptive machine learning-based redundancy prediction approach to further improve the suppression of data when any traffic pattern changes. Further work can also focus on lightweight encryption mechanisms that improve security without adding to the computational burden. Testing the model in large-scale, real-time IoT settings, such as those taking mobility into consideration, would serve as a proof of the cause of how viable it is in the real world. Moreover, application of cross-layer routing and cross-layer clustering mechanisms to RERESDA can also improve the scalability, fault tolerance of the network and enhancement of the overall network.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] B. Aggarwal, A. Akella, A. Anand, A. Balachandran, P. Chitnis, C. Muthukrishnan, R. Ramjee, and G. Varghese, "EndRE: An end-system redundancy elimination service for enterprises," in Proc. 9th USENIX Symp. Netw. Syst. Design Implement. (NSDI), San Jose, CA, USA, 2012, pp. 375–388.

[2] G. Lu, Y. Jin, and D. Du, "Frequency-based chunking for data deduplication," in Proc. IEEE Int. Symp. Model., Anal. Simul. Comput. Telecommun. Syst. (MASCOTS), 2010, pp. 287–296, doi: 10.1109/MASCOTS.2010.37.

[3] S. Saha, A. Lukyanenko, and A. Ylä-Jääski, "Combiheader: Minimizing the number of shim headers in redundancy elimination systems," in Proc. IEEE INFOCOM Workshops, 2012, pp. 798–803, doi: 10.1109/INFCOMW.2011.5928920.

[4] M. Salah ud Din, M. A. U. Rehman, R. Ullah, C.-W. Park, D. H. Kim, and B.-S. Kim, "Improving resource-constrained IoT device lifetimes by mitigating redundant transmissions across heterogeneous wireless multimedia of things," Digit. Commun. Netw., vol. 8, no. 5, pp. 778–790, 2022, doi: 10.1016/j.dcan.2021.09.004.

[5] S. Aswale and V. R. Ghorpade, "Geographic multipath routing based on triangle link quality metric with minimum inter-path interference for wireless multimedia sensor networks," J. King Saud Univ. Comput. Inf. Sci., vol. 33, no. 1, pp. 33–44, 2021, doi: 10.1016/j.jksuci.2018.02.001.

[6] G. A. Lobiyal and J. H. Abawajy, "Energy-efficient multipath routing algorithm for wireless multimedia sensor networks," Sensors, vol. 19, no. 17, p. 3642, 2019, doi: 10.3390/s19173642.

[7] G. P. Raja and S. Mangai, "Firefly load balancing based energy optimized routing for multimedia data delivery in wireless mesh network," Cluster Comput., vol. 22, no. S5, pp. 12077–12090, 2019, doi: 10.1007/s10586-017-1557-1.

[8] F. H. Awad, "Optimization of relay node deployment for multisource multipath routing in wireless multimedia sensor networks using Gaussian distribution," Comput. Netw., vol. 145, pp. 96–106, 2018, doi: 10.1016/j.comnet.2018.08.021.

[9] M. A. Habib and S. Moh, "Robust evolutionary-game-based routing for wireless multimedia sensor networks," Sensors, vol. 19, no. 16, p. 3544, 2019, doi: 10.3390/s19163544.
[10] Y. Tripathi, A. Prakash, and R. Tripathi, "Load-aware multipath data forwarding for enhanced lifetime of wireless sensor networks," Int. J. Inf. Technol., vol. 13, pp. 807–815, 2021, doi: 10.1007/s41870-020-00557-y.
[11] C. Xu, Z. Xiong, G. Zhao, and S. Yu, "An energy-efficient region source routing protocol for lifetime maximization in wireless sensor networks," IEEE Access, vol. 7, pp. 135277–135289, 2019, doi: 10.1109/ACCESS.2019.2942321.
[12] S. Govindaraj and S. N. Deepa, "Network energy optimization of IoTs in wireless sensor networks using capsule neural network learning model," Wireless Pers. Commun., vol. 115, pp. 2415–2436, 2020, doi: 10.1007/s11277-020-07688-2.
[13] S. Ambareesh and A. N. Madheswari, "HRDSS-WMSN: A multi-objective function for optimal routing protocol in wireless multimedia sensor networks using hybrid red deer–SALP swarm algorithm," Wireless Pers. Commun., vol. 119, pp. 117–146, 2021, doi: 10.1007/s11277-021-08201-z.
[14] A Gutub, "Boosting image watermarking authenticity spreading secrecy from counting-based secret sharing," CAAI Trans. Intell. Technol., 2022, doi: 10.1049/cit2.12093.
[15] Z. Chen, "Internet security situation awareness prediction based on improved RBF neural network," J. Comput. Cogn. Eng., vol. 1, pp. 103–108, 2022, doi: 10.47852/bonviewJCCE149145205514.
[16] P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," Future Gener. Comput. Syst., vol. 83, pp. 629–637, 2018, doi: 10.1016/j.future.2017.06.023.
[17] A Wani and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier," CAAI Trans. Intell. Technol., vol. 6, pp. 281–290, 2021, doi: 10.1049/cit2.12003.
[18] S. Das and S. Namasudra, "A lightweight and anonymous mutual authentication scheme for medical big data in distributed smart healthcare systems," IEEE/ACM Trans. Comput. Biol. Bioinform., early access, 2022, doi: 10.1109/TCBB.2022.3230053.
[19] R. Verma, A. Kumari, A. Anand, and V. S. S. Yadavalli, "Revisiting shift cipher technique for amplified data security," J. Comput. Cogn. Eng., 2022, doi: 10.47852/bonviewJCCE2202261.
[20] S. Sarkar, K. Saha, S. Namasudra, and P. Roy, "An efficient and time-saving web service-based Android application," SSRG Int. J. Comput. Sci. Eng., vol. 2, no. 8, pp. 18–21, 2016, doi: 10.14445/23488387/IJCSE-V2I8P104.
[21] A Kumar, P. Singh, and R. Kumar, "Energy-efficient secure data aggregation for clustered wireless sensor networks," IEEE Access, vol. 12, pp. 34567–34579, 2024.
[22] L. Zhang, Y. Liu, and H. Wang, "Redundancy-aware data aggregation using temporal correlation in wireless sensor networks," Sensors, vol. 24, no. 3, pp. 1121–1136, 2024.
[23] M. Elhoseny, K. Shankar, and A. K. Sangaiah, "Lightweight secure aggregation scheme for energy-constrained wireless sensor networks," Future Gener. Comput. Syst., vol. 150, pp. 45–57, 2024.
[24] S. Verma and N. Mittal, "Energy-aware clustering and data suppression for large-scale wireless sensor networks," IEEE Sensors J., early access, 2025.
[25] J. Chen, X. Li, and Z. Zhou, "Joint redundancy elimination and secure data transmission in Internet of Things–enabled sensor networks," IEEE Internet Things J., early access, 2025.
[26] T. Nguyen, M. T. Thai, and L. Xie, "Energy-aware temporal data suppression for long-lived wireless sensor networks," IEEE Sensors J., vol. 24, no. 9, pp. 13456–13468, 2024.
[27] S. Rani, A. Sharma, and J. Rodrigues, "Secure and lightweight data aggregation for energy-constrained wireless sensor networks," IEEE Access, vol. 12, pp. 78901–78914, 2024.
[28] H. Alsharif, M. Elhoseny, and K. Shankar, "Redundancy-aware clustering and aggregation framework for large-scale wireless sensor networks," Sensors, vol. 24, no. 11, pp. 4821–4836, 2024.
[29] P. K. Singh and S. Namasudra, "Lightweight authentication and secure data aggregation for IoT-enabled sensor networks," IEEE Internet Things J., early access, 2025.
[30] Y. Zhou, J. Wang, and Q. Chen, "Joint energy optimization and redundancy elimination in clustered wireless sensor networks," IEEE Access, early access, 2025.
[31] D. B. Darshan and C. R. Prashanth, "EECRPSID: Energy-efficient cluster-based routing protocol with a secure intrusion detection for WSN-assisted IoT," International Journal of Computer Networks & Communications (IJCNC), vol. 16, no. 3, May 2024.

[32] N. Kashyap, S. Upadhyaya, M. Poriye and S. Lalar, "Fuzzy-based clustering of wireless sensor networks for multiple mobile agent itinerary planning," International Journal of Computer Networks & Communications (IJCNC), vol. 16, no. 6, Nov 2024.

AUTHORS

DR. SUNIL S. HARAKANNANAVAR is an Associate Professor in the Department of Electronics and Communication Engineering at Nitte Meenakshi Institute of Technology (NMIT), Bengaluru, with 12+ years of teaching experience and 4 years of research experience. He obtained his Ph.D. in Image and Signal Processing from VTU, Belagavi (2020), M.Tech in Microelectronics & Control Systems from NMAMIT, Nitte (VTU, 2012), and B.E. in Electronics & Communication Engineering from STJIT, Ranebennur (VTU, 2010). His research interests include signal and image processing, IoT, AI & machine learning for ECE applications, wireless networks, and biometric authentication systems, and he has published 26 journal papers and 25 conference papers in reputed venues including IEEE and Scopus-indexed proceedings. He holds 6 patents (including Australian granted patents) and has secured funded projects from agencies such as DRDO-GTRE and VGST, while also contributing as a reviewer/editorial member for reputed journals. He is an IEEE Senior Member and actively participates in professional and research.

DR. SUMATHI M. S is currently associated with the Department of Electronics & Telecommunication Engineering, BMS Institute of Technology and Management, Bengaluru, Karnataka, India. Her research interests include wireless sensor networks, distributed systems, energy-aware networking protocols, secure data transmission, and fault-tolerant network design. Her work focuses on improving the efficiency and reliability of IoT-enabled sensor networks for next-generation applications.

DR. SRINIVASAN P is currently associated with the Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Nagercoil Campus, India. His research includes wireless and multimedia sensor networks, with primary interests in routing optimization, multipath communication, and network performance analysis. His contributions address reliability enhancement, throughput improvement, and lifetime maximization in large-scale sensor network deployments.

DR. SAPNAKUMARI C is currently associated with the Department of Electronics and Communication Engineering, Sapthagiri NPS University, Bengaluru, Karnataka, India. Her research focuses on wireless sensor networks and distributed systems, emphasizing energy-efficient communication, secure data transmission, and fault-resilient network design. Her work aims to improve the performance and scalability of IoT-based sensor network infrastructures.

DR. RANGASWAMY Y is currently associated with the Department of Electronics and Communication Engineering, Dr Ambedkar Institute of Technology, Bengaluru, Karnataka, India. His research interests include wireless sensor networks, energy-aware communication frameworks, secure data delivery, and fault-tolerant network protocols. His work contributes toward improving reliability, scalability, and efficiency in next-generation IoT-enabled sensor networks.