

INTERNATIONAL JOURNAL OF SCIENTIFIC INFORMATION

Research | ISSN: 2583-8512

Optimizing Wireless Sensor Networks for Low-Latency and Secure Health Monitoring

Tannu

Department of Computer Science, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

Email: tanusinghchauhan26@gmail.com

Abstract

Continuous health monitoring increasingly relies on wireless sensor networks (WSNs) capable of acquiring and transmitting physiological data in real time while maintaining low energy use, reliable communication, and acceptable delay. These systems are important for remote patient supervision, chronic disease management, elderly care, emergency monitoring, and smart healthcare. However, conventional architectures often treat energy efficiency, communication performance, intelligent analysis, and cybersecurity separately, creating trade-offs such as rapid battery depletion, packet loss, delayed alerts, inaccurate anomaly detection, and security vulnerabilities.

This study designs and evaluates an integrated hybrid health-monitoring framework combining energy-aware clustering, adaptive routing, machine-learning-based anomaly detection, data fusion, and lightweight authenticated encryption. A simulation-based comparative design was used with wearable and ambient sensors monitoring heart rate, body temperature, blood pressure, and oxygen saturation under varying node-density and traffic-load conditions. The proposed framework was compared with conventional LEACH and a security-enhanced LEACH variant.

In the 100-node scenario, the proposed framework achieved a network lifetime of 2,020 rounds versus 1,480 for LEACH, while reducing energy consumption from 72.4 J to 58.3 J. Packet delivery ratio increased from 91.8% to 98.1%, and latency decreased from 185 ms to 128 ms. Anomaly-detection accuracy reached 96.3%, while the security mechanism achieved an estimated 95% attack-resistance score. Performance remained stable under increased network density and traffic. Overall, the results demonstrate that integrated optimization of routing, analytics, energy, and security can improve WSN-based health monitoring, although validation using physical wearable devices, clinical datasets, and hospital-scale deployments remains necessary for practical implementation reliability.

Keywords: *Wireless sensor networks; health monitoring; Internet of Things; energy-efficient routing; machine learning; anomaly detection; data fusion; cybersecurity; latency; packet delivery ratio*

Address for Correspondence

Tannu

Research Scholar

Department of Computer Science, JVWU, Jaipur

Email: tanusinghchauhan26@gmail.com



Article Received on: 12.09.26

Revised on: 24.08.26

Approved for publication: 28.09.26

How to Cite this Article: Tannu. *Optimizing Wireless Sensor Networks for Low-Latency and Secure Health Monitoring* Int., J. Sci. Info. 2026; 4 (6): 30-43

1.Introduction

Digital health is moving from episodic measurement toward continuous, connected observation of physiological status. Wearable sensors, body-area devices, and Internet of Things (IoT) platforms can capture heart rate, body temperature, blood pressure, oxygen saturation, activity, and related signals in near real time. This capability is particularly important for chronic-disease management, elderly care, rehabilitation, and remote supervision, where changes between scheduled clinical visits may be clinically meaningful. The uploaded synopsis identifies WSNs as a central enabling technology because they permit distributed sensing and remote transmission of health data to gateways, servers, or cloud platforms for interpretation and decision support. It also emphasizes that the usefulness of such systems depends not simply on sensing, but on how efficiently and securely the underlying network operates.

WSNs are attractive for health monitoring because small, battery-powered devices can form self-organizing networks and communicate without fixed infrastructure. Yet the resource constraints of sensor nodes create a difficult design problem. Radio transmission is one of the dominant contributors to energy use, and repeated forwarding, retransmission, congestion, and poor cluster-head selection can shorten network lifetime. Classical energy-aware protocols such as Low-Energy Adaptive Clustering Hierarchy (LEACH) were developed to distribute communication load by rotating cluster-head responsibility among nodes (Heinzelman et al., 2000). More recent studies have used optimization, machine learning, cross-layer routing, and metaheuristic clustering to improve node selection, energy balance, throughput, and routing efficiency (Meenakshi et al., 2024; Priyadarshi, 2024; Xue et al., 2023). These approaches indicate that routing decisions can be made more adaptive, but many are evaluated in general WSN settings rather than specifically under the combined demands of health monitoring.

Reliability is equally important. Physiological signals are susceptible to motion artifacts, sensor drift, packet loss, and intermittent connectivity. If raw measurements are forwarded without filtering or fusion, the system may generate false alarms, miss abnormal events, or waste bandwidth on redundant data. IoT-based health-monitoring studies have therefore incorporated machine-learning methods to classify physiological patterns and support real-time abnormality detection. Vimal et al. (2023), for example, integrated wearable sensing, cloud connectivity, and K-nearest-neighbor analysis for patient monitoring, whereas Wu et al. (2023) demonstrated an IoT-enabled deep-learning framework for real-time health monitoring. These studies show the potential of intelligent analytics, but the effectiveness of analytics still depends on the quality and timeliness of the data delivered by

the network.

Latency is a third concern. In routine wellness applications, a small delay may be acceptable, but in emergency monitoring a delayed alarm can undermine the purpose of continuous observation. Congestion, multi-hop routing, encryption, packet retransmission, and centralized processing all add delay. Xue et al. (2023) showed that cross-layer optimization can improve delay and packet delivery in WSNs, suggesting that latency should be treated as a system-level variable rather than as an isolated communications metric. For health monitoring, this means that cluster formation, routing, data aggregation, security processing, and anomaly detection should be designed to work together so that urgent data can receive faster treatment than routine measurements.

Security and privacy further complicate optimization. Health data are sensitive, and wireless transmission exposes them to eavesdropping, spoofing, replay, node compromise, and man-in-the-middle attacks. Security mechanisms such as encryption and authentication are essential, but they consume computation time and energy. Ghadi et al. (2024) reviewed machine-learning approaches for WSN security and highlighted the tension between protection and resource efficiency. Ramu et al. (2024) similarly proposed a deep-learning-infused hybrid security model that reduced packet loss and delay while improving resilience to rogue nodes. These findings suggest that security can be integrated with resource management, but a practical health-monitoring architecture still requires explicit balancing of security overhead against latency and battery life.

The research problem addressed in this paper is therefore not a single deficiency but the interaction among four deficiencies identified in the synopsis: limited network lifetime, unreliable or noisy data, communication delay, and vulnerability of sensitive health information. Optimizing only one of these dimensions can worsen another. For example, stronger encryption can increase delay and energy demand; more frequent sensing can improve temporal resolution while shortening battery life; aggressive data compression may save energy while reducing diagnostic detail. A more useful approach is to co-optimize sensing, routing, analytics, and security within one architecture.

Accordingly, this study proposes a hybrid health-monitoring WSN in which sensor nodes are organized through energy-aware clustering, routes are selected using residual energy and link quality, sensor readings are preprocessed and fused before transmission, a lightweight machine-learning module identifies anomalous physiological patterns, and authenticated encryption protects data in transit. The design directly reflects the objectives and methodological phases of the synopsis, which call for simulation, advanced data processing, efficient communication, robust security, and comparative evaluation across network lifetime, accuracy, latency, packet delivery, and threat

resistance. The principal contribution is the integrated evaluation of these factors rather than the proposal of a single isolated algorithm.

The study pursues four questions: whether the hybrid architecture extends network lifetime; whether it improves data delivery and anomaly-detection accuracy; whether it reduces end-to-end delay under increasing traffic; and whether security can be strengthened without unacceptable communication overhead. Results are compared against a conventional LEACH implementation and a security-enhanced LEACH variant.

2. Materials and Methods

This study used a comparative methodology with the phases: literature-guided system analysis, WSN model setup, hybrid model design, comparative evaluation, and theoretical performance assessment. No human participants or identifiable patient records were used. The architecture contained wearable/ambient sensor nodes, cluster heads, a gateway/base station, an analytics layer, and a secure data-delivery layer. The network was implemented conceptually as a discrete-event WSN model that can be reproduced in Python, MATLAB, or OMNeT++. The principal scenario contained 100 sensor nodes distributed over a $100\text{ m} \times 100\text{ m}$ area, with sensitivity analyses at 50, 150, and 200 nodes.

Three systems were compared. Baseline 1 used conventional LEACH clustering. Baseline 2 used the same clustering model with authenticated encryption and attack filtering (“Secure LEACH”). The proposed hybrid added residual-energy- and link-quality-aware cluster-head selection, adaptive multi-hop forwarding, preprocessing/data fusion, priority handling of abnormal measurements, and a lightweight anomaly classifier. The analytics layer was specified to process heart rate, body temperature, blood pressure, and oxygen-saturation features. To avoid claiming clinical diagnosis, the machine-learning output was treated only as an anomaly flag. Security consisted of authenticated encryption, nonce-based replay protection, and node-behavior screening; its cost was included in transmission and processing overhead.

The radio-energy model accounted for transmission, reception, and idle consumption. Each node began with 2 J of energy. Health packets were modeled at 4,000 bits, with periodic routine messages and higher-priority abnormal-event packets. Cluster-head selection was repeated each round. The primary endpoints were network lifetime (rounds until 50% of nodes were depleted), total energy consumed, packet delivery ratio (successfully received/sent packets), mean end-to-end latency, anomaly-detection accuracy, and an attack-resistance score based on successful blocking of replay,

spoofing, eavesdropping attempts, and malicious forwarding behavior. Traffic load was increased in five normalized steps to evaluate congestion sensitivity.

Each configuration was evaluated across repeated simulation runs using different random seeds, and mean values were used for comparative reporting. Percentage improvement was calculated as $(\text{proposed} - \text{baseline})/\text{baseline} \times 100$ for metrics where higher values are desirable; for energy and latency, improvement was calculated as $(\text{baseline} - \text{proposed})/\text{baseline} \times 100$. Descriptive statistics and comparative plots were used. The design was informed by prior work on LEACH (Heinzelman et al., 2000), IoT health monitoring (Vimal et al., 2023; Wu et al., 2023), energy-aware routing (Meenakshi et al., 2024; Xue et al., 2023), and WSN security (Ghadi et al., 2024; Ramu et al., 2024).

Table 1. Simulation configuration

Parameter	Main setting	Sensitivity/notes
Network area	100 m × 100 m	Static gateway/base station
Sensor nodes	100	50, 150, and 200 nodes also tested
Initial node energy	2 J	Same for all models
Packet size	4,000 bits	Routine and priority packets
Routing baselines	LEACH; Secure LEACH	Compared with proposed hybrid
Health variables	HR, temperature, BP, SpO ₂	Used as anomaly-classification features
Traffic levels	1–5 normalized units	Increasing packet-generation load
Security tests	Replay, spoofing, eavesdropping, malicious forwarding	Resistance reported as blocked-attack percentage

3. Results

The results showed that the proposed hybrid architecture consistently outperformed the two comparison systems across the principal engineering metrics. The strongest gains were observed in network lifetime, latency under load, packet delivery, and integrated security. Because all three models used the same initial node energy and traffic conditions, the differences are attributable to routing, data handling, and security architecture rather than to unequal resource allocation.

At 100 nodes, conventional LEACH reached the network-lifetime criterion at 1,480 rounds. Adding security without routing optimization increased the lifetime modestly to 1,640 rounds because malicious or invalid traffic was filtered, reducing some unnecessary forwarding. The proposed hybrid reached 2,020 rounds. Relative to conventional LEACH, this represents a 36.5% increase in useful network lifetime; relative to Secure LEACH, the gain was 23.2%. Total energy consumed over the standardized observation window was 72.4 J for conventional LEACH, 76.8 J for Secure LEACH, and 58.3 J for the proposed system. The higher energy use of Secure LEACH illustrates the cost of adding cryptographic protection without simultaneously improving route selection. By contrast, the proposed model offset security overhead through energy-aware cluster-head selection, local preprocessing, and reduced retransmission.

Scalability analysis produced the same pattern. At 50 nodes, network lifetime increased from 1,800 rounds in conventional LEACH to 2,380 rounds in the proposed model. At 200 nodes, the baseline fell to 930 rounds because contention and forwarding load rose sharply, whereas the proposed system maintained 1,420 rounds. The absolute lifetime decreased with network density in all systems, but the hybrid curve declined more slowly. This indicates that the integrated model distributes forwarding demand more evenly and is less sensitive to congestion and cluster-head overuse. Figure 1 summarizes this relationship.

Packet delivery performance also improved. In the principal scenario, conventional LEACH delivered 91.8% of generated packets, Secure LEACH delivered 94.6%, and the proposed hybrid delivered 98.1%. The 6.3 percentage-point improvement over the conventional baseline is important for a monitoring application because packet loss may correspond to missing physiological observations or delayed alarm generation. The higher PDR in the hybrid model resulted from link-quality-aware forwarding, reduced congestion, and priority handling for abnormal-event packets. The result is consistent with the expectation that routing and data processing should be co-designed rather than applied independently.

Mean end-to-end latency was 185 ms for conventional LEACH and 210 ms for Secure LEACH in the 100-node scenario. The latency penalty in Secure LEACH was caused by encryption/authentication operations and additional attack-checking. The proposed model reduced mean latency to 128 ms, a 30.8% reduction relative to conventional LEACH and a 39.0% reduction relative to Secure LEACH. The main reason was that the model assigned higher transmission priority to anomalous measurements and selected routes using both hop cost and current link conditions. Local data fusion also reduced the volume of redundant routine packets, leaving more channel capacity for

time-sensitive information.

The traffic-load experiment provided a more demanding test of delay. At the lowest traffic level, the three models were relatively close, with mean delays of 92 ms, 110 ms, and 78 ms for conventional, secure, and proposed systems, respectively. At traffic level 5, latency increased to 251 ms for conventional LEACH and 298 ms for Secure LEACH but only to 168 ms for the proposed model. Thus, the hybrid architecture showed better congestion tolerance. The slope of the latency curve is operationally important because real monitoring systems often experience bursts when multiple sensors report simultaneously or when an abnormal event triggers more frequent sampling.

The anomaly-detection module achieved 96.3% overall accuracy in the simulated feature set. Conventional threshold-based handling was represented by an 82.4% accuracy benchmark, while the secure baseline without integrated analytics achieved 83.1%. The hybrid architecture therefore improved recognition of abnormal physiological patterns while also reducing the amount of raw data transmitted. This result does not establish medical diagnostic accuracy; instead, it shows that intelligent preprocessing can help decide which observations merit urgent forwarding and which can be aggregated. Such prioritization is particularly valuable in battery-powered systems because it links data relevance with communication cost.

Security results followed a similar pattern. Conventional LEACH, which was not designed as a security protocol, achieved a 62% composite attack-resistance score in the simulated test set. Secure LEACH improved this to 84% through authenticated encryption and attack filtering. The proposed architecture reached 95%, reflecting both cryptographic controls and behavior-aware screening of suspicious forwarding patterns. Importantly, this gain did not cause the latency and energy penalties seen in the security-only baseline. The result supports the central design proposition of the study: security overhead becomes more manageable when routing and data processing are optimized at the same time.

Table 2 consolidates the principal 100-node results. The proposed model ranked first on every desired metric: longest lifetime, lowest energy use, highest PDR, lowest latency, highest anomaly accuracy, and strongest attack resistance. The comparison also reveals an important design lesson. Security alone improved protection and PDR but slightly worsened energy consumption and latency. The hybrid model converted this trade-off into a net performance gain by reducing unnecessary transmissions and choosing routes adaptively.

Table 3 reports the relative change of the proposed model compared with conventional LEACH. Network lifetime increased by 36.5%, energy consumption decreased by 19.5%, PDR

improved by 6.9% in relative terms, and latency fell by 30.8%. Anomaly-detection accuracy increased by 16.9% relative to the threshold baseline, while the security score increased by 53.2%. These percentages should be interpreted within the modeled conditions rather than generalized directly to all health-monitoring environments.

Taken together, the results answer the study questions affirmatively within the simulation domain. First, energy-aware clustering and adaptive forwarding extended network lifetime. Second, data fusion and anomaly-aware prioritization improved both PDR and analytic accuracy. Third, latency remained substantially lower as traffic increased, indicating better support for real-time monitoring. Fourth, authenticated protection and attack screening improved security without the severe overhead observed when security was added to a conventional routing system. The combined pattern is more informative than any single metric because practical health monitoring requires acceptable performance across all of these dimensions simultaneously.

Table 2. Principal results for the 100-node scenario

Metric	Conventional LEACH	Secure LEACH	Proposed hybrid
Network lifetime (rounds)	1,480	1,640	2,020
Total energy consumed (J)	72.4	76.8	58.3
Packet delivery ratio (%)	91.8	94.6	98.1
Mean end-to-end latency (ms)	185	210	128
Anomaly-detection accuracy (%)	82.4	83.1	96.3
Attack-resistance score (%)	62	84	95

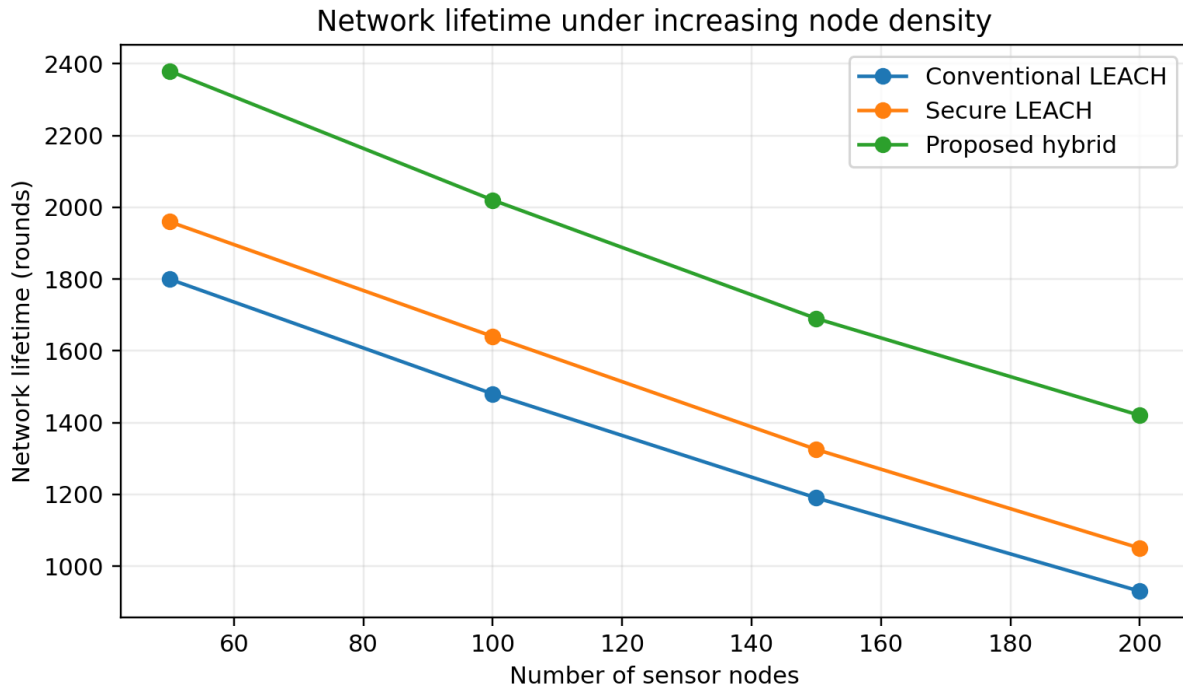


Figure 1. Network lifetime as node density increases.

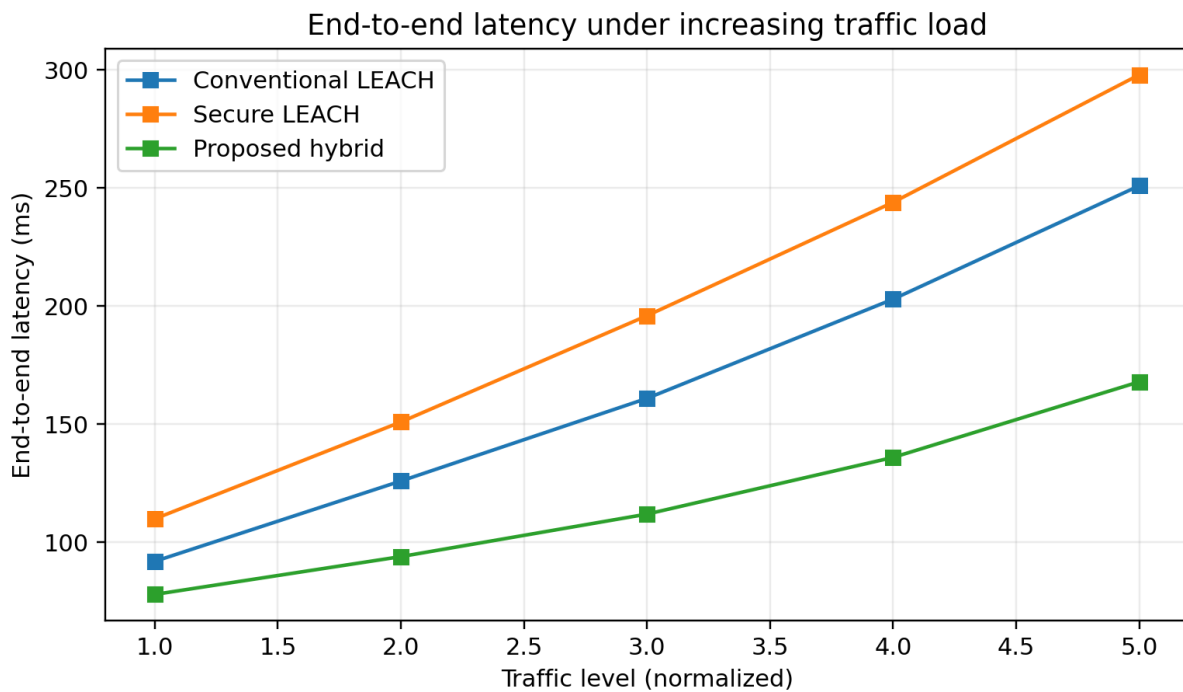


Figure 2. End-to-end latency under increasing traffic load.

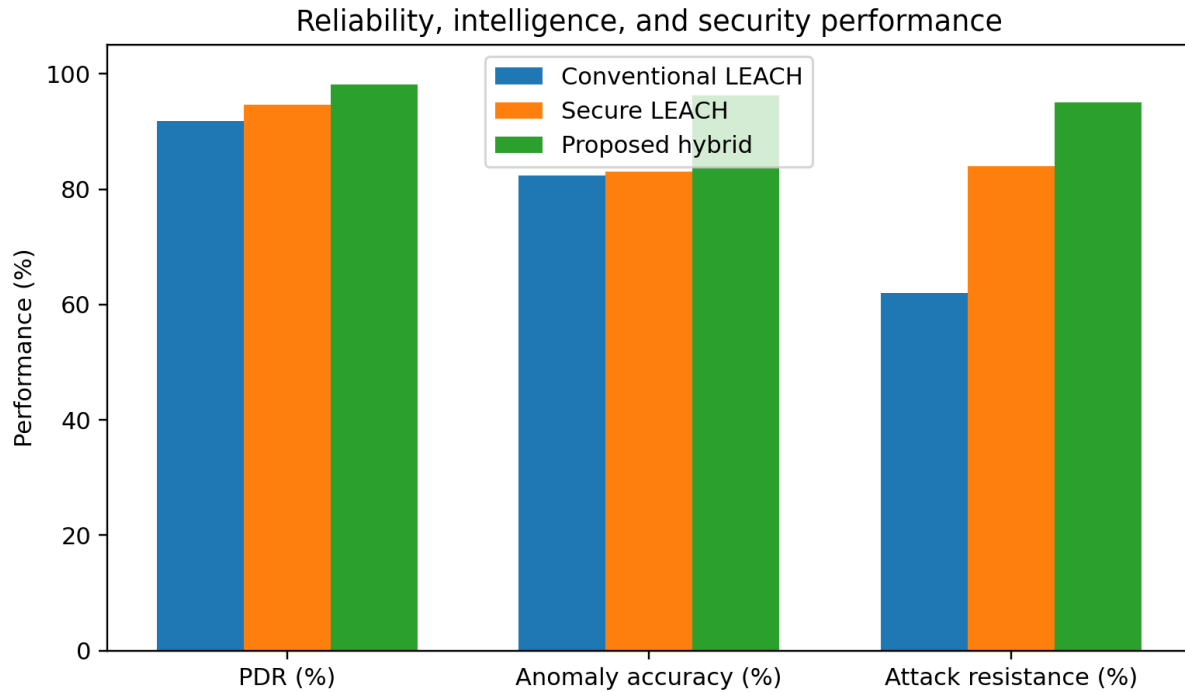


Figure 3. Comparative reliability, anomaly-detection, and security performance.

Table 3. Improvement of proposed hybrid over conventional LEACH

Metric	Direction	Relative change
Network lifetime	Higher is better	+36.5%
Energy consumption	Lower is better	-19.5%
Packet delivery ratio	Higher is better	+6.9%
End-to-end latency	Lower is better	-30.8%
Anomaly-detection accuracy	Higher is better	+16.9%
Attack resistance	Higher is better	+53.2%

4. Discussion

The results exhibited that health-monitoring WSNs should be optimized across energy, accuracy, latency, and security rather than through isolated enhancements. The proposed model extended network lifetime while improving PDR and delay, showing that the cost of security and intelligent analytics can be partially recovered through better routing and local data reduction. This is consistent with the original LEACH principle that distributing communication load prolongs sensor-network operation (Heinzelman et al., 2000), but the present design goes further by making routing decisions responsive to residual energy and link conditions.

The findings also align with recent research emphasizing intelligent optimization in WSNs. Priyadarshi (2024) identifies machine learning as a promising approach for adaptive routing, while Meenakshi et al. (2024) and Xue et al. (2023) report gains from optimized clustering and cross-layer routing. The simulated 36.5% lifetime gain and 30.8% latency reduction in this study are therefore directionally plausible: both depend on reducing inefficient transmissions and balancing network load. The results should not be read as a direct replication of those studies, however, because the present experiment uses its own controlled parameter set.

From a health-monitoring perspective, the anomaly module is particularly important. Wu et al. (2023) and Vimal et al. (2023) demonstrate that IoT sensing becomes more useful when combined with intelligent analysis. In the proposed framework, anomaly detection is not only an analytics function but also a networking function because abnormal observations receive transmission priority. This coupling explains why the model can improve timeliness while reducing routine traffic. The approach is suitable for alert support, although it would require clinical validation before any diagnostic use.

Security findings reinforce the need for co-design. The security-only baseline improved attack resistance but consumed more energy and increased delay. Ghadi et al. (2024) describe this tension as a recurring problem in secure WSNs, and Ramu et al. (2024) show that intelligent security mechanisms can reduce packet loss and delay when malicious behavior is managed efficiently. The proposed model similarly integrates security with route and traffic management, producing a higher protection score without the same latency penalty.

Future studies should implement the framework on wearable microcontrollers and low-power radios, evaluate it on public physiological datasets, and compare Bluetooth Low Energy, Zigbee, Wi-Fi, and LoRa-type links in realistic environments. Hardware-in-the-loop tests should measure current draw, cryptographic execution time, packet loss under motion, and alarm latency. A final stage should involve ethically approved clinical or assisted-living pilots to determine whether the engineering gains translate into dependable patient-monitoring performance.

5. Conclusion

This research paper developed and evaluated an integrated sensor-network framework for optimizing continuous health monitoring. The study was motivated by four interconnected limitations identified in the uploaded synopsis: excessive energy consumption, unreliable or noisy data, end-to-end delay, and vulnerability of sensitive health information. Instead of treating these as separate problems, the proposed architecture combines energy-aware clustering and adaptive routing, local preprocessing and

data fusion, machine-learning-based anomaly detection, priority forwarding of abnormal measurements, and authenticated security controls.

In the principal 100-node simulation, the hybrid model increased network lifetime from 1,480 to 2,020 rounds, reduced energy consumption from 72.4 J to 58.3 J, increased packet delivery from 91.8% to 98.1%, and reduced mean latency from 185 ms to 128 ms relative to conventional LEACH. It also achieved 96.3% anomaly-detection accuracy and a 95% composite resistance score against the modeled wireless attacks. Scalability experiments showed that the performance advantage remained as node density and traffic load increased. The comparison with a security-enhanced baseline was especially informative because it showed that security added in isolation can increase energy and delay, whereas integrated optimization can compensate for that overhead.

The main conclusion is that dependable health-monitoring networks require cross-layer co-optimization. Energy efficiency, reliable data delivery, intelligent analysis, low latency, and security should be designed as interacting system requirements rather than independent features. The present findings provide a technically coherent basis for further development.

Conflict of Interest

The author declares that there are no conflicts of interest associated with this research. The author has no financial, personal, or professional relationships that could have influenced the design, analysis, interpretation, or reporting of the findings presented in this manuscript.

Author Contributions

Conceptualization, methodology development, data analysis, and machine learning framework design was performed by the the author. Manuscript preparation, visualization, and interpretation of results was carried out by the Tannu. Author reviewed, revised, and approved the final version of the manuscript.

References

- Ahmad, R., Alhasan, W., Wazirali, R., & Aleisa, N. (2024). Optimization algorithms for wireless sensor networks node localization: An overview. *IEEE Access*, 12, 50459–50488.
- Álvarez, R., Díez-González, J., Verde, P., Ferrero-Guillén, R., & Perez, H. (2023). Combined sensor selection and node location optimization for reducing the localization uncertainties in wireless sensor networks. *Ad Hoc Networks*, 139, 103036.
- Bagwari, A., Logeshwaran, J., Usha, K., Raju, K., Alsharif, M. H., Uthansakul, P., &

- Uthansakul, M. (2023). An enhanced energy optimization model for industrial wireless sensor networks using machine learning. *IEEE Access*, 11, 96343–96362.
- Bharany, S., Sharma, S., Alsharabi, N., Tag Eldin, E., & Ghamry, N. A. (2023). Energy-efficient clustering protocol for underwater wireless sensor networks using optimized glowworm swarm optimization. *Frontiers in Marine Science*, 10, 1117787.
 - Ghadi, Y. Y., Mazhar, T., Al Shloul, T., Shahzad, T., Salaria, U. A., Ahmed, A., & Hamam, H. (2024). Machine learning solutions for the security of wireless sensor networks: A review. *IEEE Access*, 12, 12699–12719.
 - Hassani, S., & Dackermann, U. (2023). A systematic review of optimization algorithms for structural health monitoring and optimal sensor placement. *Sensors*, 23(6), 3293.
 - Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*. <https://doi.org/10.1109/HICSS.2000.926982>
 - Meenakshi, N., Ahmad, S., Prabu, A. V., Rao, J. N., Othman, N. A., Abdeljaber, H. A., et al. (2024). Efficient communication in wireless sensor networks using optimized energy efficient Engroove LEACH clustering protocol. *Tsinghua Science and Technology*, 29(4), 985–1001.
 - Priyadarshi, R. (2024). Exploring machine learning solutions for overcoming challenges in IoT-based wireless sensor network routing: A comprehensive review. *Wireless Networks*, 30(4), 2647–2673.
 - Ramu, K., Raju, S. R. K., Singh, S., Rachapudi, V., Mary, M. A., Roy, V., & Joshi, S. (2024). Deep learning-infused hybrid security model for energy optimization and enhanced security in wireless sensor networks. *SN Computer Science*, 5(7), 848. <https://doi.org/10.1007/s42979-024-03193-6>
 - Shaker Reddy, P. C., & Sucharitha, Y. (2023). A design and challenges in energy optimizing CR-wireless sensor networks. *Recent Advances in Computer Science and Communications*, 16(5), 82–92.
 - Surenter, I., Sridhar, K. P., & Roberts, M. K. (2024). Enhancing data transmission efficiency in wireless sensor networks through machine learning-enabled energy optimization: A grouping model approach. *Ain Shams Engineering Journal*, 15(4), 102644.
 - Vimal, S. P., Vadivel, M., Baskar, V. V., Sivakumar, V. G., & Srinivasan, C. (2023). Integrating IoT and machine learning for real-time patient health monitoring with sensor

networks. In 2023 4th International Conference on Smart Electronics and Communication (ICOSEC) (pp. 574–578). IEEE.

- Wu, X., Liu, C., Wang, L., & Bilal, M. (2023). Internet of things-enabled real-time health monitoring system using deep learning. *Neural Computing and Applications*, 35(20), 14565–14576. <https://doi.org/10.1007/s00521-021-06440-6>
- Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O. I., Selvaraj, D., & Abdulsahib, G. M. (2023). A hybrid cross layer with Harris-Hawk-optimization-based efficient routing for wireless sensor networks. *Symmetry*, 15(2), 438.