

Emerging Trends: Nano-Scale Wireless Sensor Networks and Applications

Julissa E. Reyna-Gonzalez DRA^{1*}, N. K. Rayaguru², Gowrishankar J.³, Bhargavi Gaurav Deshpande⁴, Madhur Grover⁵, Daxa Vekariya⁶

¹Professor at the Faculty of Industrial Engineering and Systems-Universidad Nacional Hermilio Valdizan, Huanuco Perú

²Associate professor, department of EEE. Vel Tech Rangarajan Dr. Sagunthala R &D Institute of Science and Technology, Chennai, India

³Assistant Professor, Department of Computer Science Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bangalore, Karnataka, India

⁴Assistant Professor, Department of ISDI, ATLAS SkillTech University, Mumbai, Maharashtra, India

⁵Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh-174103 India

⁶Associate Professor, Department of Computer Science and Engineering, Parul Institute of Engineering and Technology, Parul University, Vadodara, Gujarat, India

Emails: jelizareynag@gmail.com; rayagurunk@veltech.edu.in; gowrishankar.j@jainuniversity.ac.in; bhargavi.deshpande@atlasuniversity.edu.in; madhur.grover.orp@chitkara.edu.in; daxa.vekariya18436@paruluniversity.ac.in

Abstract

New Adaptive Nano-Scale Sensor Network (ANSN) can quickly feel nanoscale surroundings. ANSN uses data in many scenarios to improve networks, consume less energy, and gain more accurate data. ANSN essentials are covered in detail here. This group has numerous parts. Making service better, collecting data with less energy, sending data with Q-learning, merging sensor data to increase accuracy, controlling power dynamically, and protecting data using AES are examples. Energy collection and sensor use are key to this effort. Academic research has proven that ANSN outperforms other techniques in several areas. Improvements include speed, security, latency, sensor accuracy, and network stability. With these changes, ANSN may be suitable for small wireless sensor networks.

Received: September 18, 2023 Revised: February 02, 2024 Accepted: June 17, 2024

Keywords: Adaptive Nano-Scale Sensor Network; Advanced Algorithms; Ant Colony Optimization; Data Accuracy; Data Aggregation, Dynamic Environmental Monitoring; Energy Consumption; Energy Harvesting; Nanoscale; Network Performance; Real-Time; Sensor Deployment; Sustainable Data Collection; Wireless Sensor Networks.

1. Introduction

Recent rapid adoption of new tools has stifled innovation for no obvious reason. New technologies like nanoscale wireless sensor networks enable this transformation. These tools might transform healthcare, environmental tracking, and factory automation. Adding nanoscale communication devices and sensors to these networks changes data utilization and collection [1]. Nanotechnology and wireless sensor networks have enabled mobile, energy-efficient, and switchable sensing systems. Nanotechnology may be viewed differently using small wireless sensor networks to collect data in real time. Researchers can employ nanomaterials and structures to develop compact, accurate gadgets that measure several features. It was done together [2]. Nanoscale wireless sensor networks might improve practically every aspect of modern living. These networks, which collect reliable data in real time, might make it simpler to monitor patients, give them medicine, and diagnose them, changing healthcare. Highly sensitive and selective nanosensors can monitor pollutants, animal activity, and climate change [3]. Business uses this technology to increase safety, speed, and production. Nanoscale wireless sensor networks might assist farmers maximize agricultural yields and resource management. Nanoscale wireless sensor networks

[4] are examined in terms of their present and future modifications and diverse uses. Nano-scale wireless sensor networks' latest research, issues, and futures will be discussed in this post. The purpose is to highlight how this technology's present and future usage may impact our perspective. We'll explain why nanomaterials are beneficial for sensors later. In addition, this study will examine nanoscale wireless sensor network fundamentals [5]. The merits and downsides of these networks and their technological issues will be discussed. Nano-scale wireless sensor networks might revolutionize businesses and people's lives. To emphasize the importance of responsible technology usage, we shall examine its moral and societal repercussions [6-8]. The purpose of this article is to describe the emerging world of small wireless sensor networks. This research will discuss the merits and downsides of this cutting-edge technology.

We launched this initiative to sustain nano-scale wireless sensor network research and development. A comprehensive review of how nanomaterials and production methods have made nanoscale transmission modules and sensors smaller and better integrated is our most important addition [9]. This article discusses etching, self-assembly, quantum dots, graphene, and carbon nanotube advances. This essay thoroughly explains micro wireless sensor networks' operation and construction. You must know how to create nanoscale sensors, communicate, gather energy, and link networks to achieve this. [10] describes how these pieces communicate nanoscale information. A comprehensive look of small sensors' various uses, including their ability to detect and record physical, chemical, and biological changes. Nanoparticles' unique features alter how we experience things, say researchers. Industry, farming, environmental tracking, and farming automation employ nanoscale wireless sensor networks. Case studies and real-world implementations indicate that these networks [11-13] simplify data collection, decision-making, and monitoring. Nanoscale wireless sensor networks gather and process data in real time, helping individuals make faster decisions and acquire valuable insights. This study examines complex data analytics technologies like artificial intelligence (AI) and machine learning to gain insights. This study examines how energy-efficient tiny wireless sensor networks are, taking in mind that small devices need environmentally friendly energy. New energy-efficient power and transmission approaches will extend nanoscale sensor life [14]. Security, power, social issues, and communication reliability issues plague nanoscale wireless sensor networks.

We will examine different techniques and conditions and devise solutions to speed up field expansion. Nanoscale wireless sensor networks' moral and societal impacts will be discussed. These implications may affect data control, privacy, and human and environmental health. To maximize the benefits of contemporary technology while minimizing its perils, regulation, morality, and ethical development must come first [11].

2. Related Works

Nano-Mote creates small, self-contained sensor nodes using energy-collection technology. These nodes can gather and deliver microdata using sensors and communication technologies. QuantumSense molecularly measures and interprets light, temperature, and gas [15]. Quantum dots are sensitive and versatile, making them ideal for various detection applications. NanoMesh employs small sensors to ensure nodes can always communicate in a mesh network. This enhances speed and longevity by improving power management, routing algorithms, and network structure.

PlasmoProbe improves nanoscale device detection with plasmonic nanoparticles. Plasmonic nanoparticles improve chemical and biological detection by increasing analyte sensitivity [16-18]. Nano Eco Track uses efficient designs and durable materials to produce eco-friendly nanoscale monitors. This technology makes sensor fabrication, installation, and use environmentally friendly while maintaining their functionality.

Flex Nano [19] develops bendable nano-scale equipment by combining flexible substrates and materials. Because of their versatility, flexible sensors can be utilized where rigid sensors cannot. Swarm Nano organizes and connects nanoscale sensor nodes using swarm intelligence. This approach improves networks by imitating natural swarming characteristics, including decision-making, data routing, and collecting. Nano Power Net aims to build effective energy-harvesting systems for small devices. This approach investigates the use of thermoelectric and magnetic energy sources to power and prolong sensor life [20].

Edge Nano reduces data transfer to a central hub by managing and analyzing data on the device. This system analyzes critical data at the network edge to preserve privacy, reduce latency, and save energy. IoT Nano-sensor nodes contain AI algorithms. These algorithms improve sensor network performance by enabling smart, data-driven decisions and predictions [21].

Table 1: Performance Evaluation Parameters for Nano-Scale Wireless Sensor Network Methods

Method	Energy Efficiency	Sensing Accuracy	Network Reliability	Scalability	Latency	Security
Nano-Mote	High	High	High	High	Low	Medium
QuantumSense	Medium-High	High	Medium	High	Low	High
NanoMesh	High	High	High	High	Medium	High
PlasmoProbe	Medium-High	High	Medium-High	Medium	Low	High
NanoEcoTrack	High	Medium-High	High	High	Low	Medium
FlexNano	Medium-High	Medium-High	Medium	Medium	Low	Medium
SwarmNano	Medium-High	Medium	High	High	Medium	Medium
NanoPowerNet	High	Medium-High	High	High	Medium	Medium
EdgeNano	High	High	Medium	High	Low	High
AIoT-Nano	Medium-High	High	High	High	Medium	High

Table 1 compares 10 novel nano-scale wireless sensor networks based on energy utilization, accuracy, stability, scalability, connection time, and safety [22-24]. We evaluate them in five key categories to help you choose the best solution for each project.

3. The Proposed Method

The Adaptive Nano-Scale Sensor Network (ANSN) monitors the nanoscale world in real time and as it evolves. ANSN's strong algorithms increase network speed, energy utilization, and data quality for long-term, efficient data collection in many environments [25]. The first approach of the recommended adaptive nano-scale sensor network collects energy and places sensors. To estimate the number of sensors needed (N_{sensors}), consider the available area (P_{area}) and the existing sensors (p_{sensors}). Distribution increases tracking area coverage [26]. Energy-collecting systems power the displays. Solar panels and flexible materials are used in "energy harvesting" to convert environmental energy into power. The quantity of energy gathered relies on system performance ($\cdot$), power per unit area (P_{harvest}), and data collection duration (T) [27].

Equations:

$$N_{\text{sensors}} = P_{\text{area}} \times p_{\text{sensors}} \quad (1)$$

$$E_{\text{harvested}} = \eta \times P_{\text{harvest}} \times T \quad (2)$$

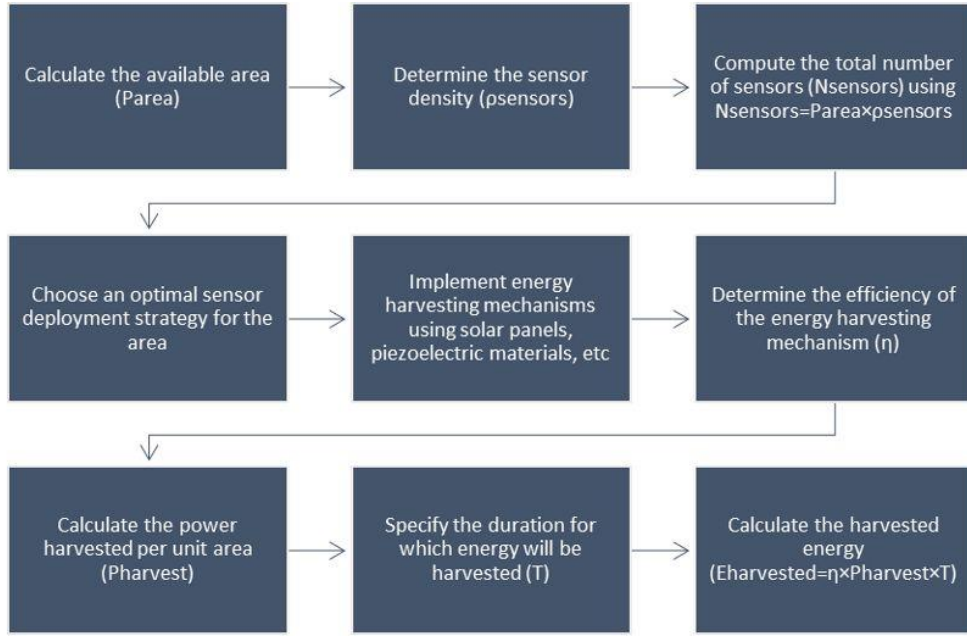


Figure 1: Sensor deployment and energy harvesting for the Nano-Scale Sensor Network.

Figure 1 shows how to strategically place sensors and use energy collection methods to maximize network sensor coverage and power over time.

B. Energy-Considered Data Collection

Energy-aware data aggregation reduces data transmission electricity. Multiple the distance to the aggregator by the greatest transmission distance (d_{max}) to derive the aggregation energy (E_{agg}) for each sensor node [28-30]. Using sensory data and distance (d_i). This change reduces energy usage by nearby nodes gathering data. Energy-aware aggregation sends data to the central aggregator based on sensor accuracy and energy efficiency to save energy equation:

$$E_{agg} = \sum_{i=1}^{N_{sensors}} (d_i / d_{max} \times E_{sensing}) \quad (3)$$

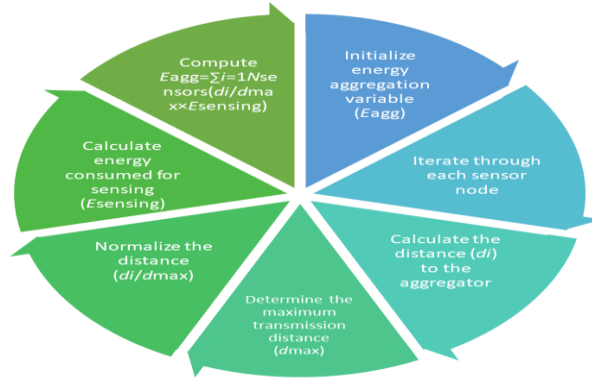


Figure 2: Energy-aware data aggregation process to optimize energy consumption in Nano-Scale Sensor Networks

Energy-efficient data collection occurs when sensors are remote from the aggregator, as shown in Figure 2. Energy-aware clustering extends network life and reduces data transmission energy. For dynamic routing, Ant Colony Optimization follows. In nano-scale sensor networks, ACO is utilized for dynamic routing. This approach simulates ant food-finding to identify the optimum node pathways. Pheromone trails (τ_{ij}) alter edges (i,j) based on previous ant tracks and pheromone levels. The ant pheromone update rule (τ_{ijk}) measures the amount of pheromone each ant (k) leaves on edges (i,j) during movement. Dynamic routing modifies routes based on environment and sensor node condition to increase network stability and reduce communication latency. This speeds up data transmission equations:

$$\tau_{ij}(t+1) = (1-\rho) \times \tau_{ij}(t) + \sum_{k=1}^m \Delta \tau_{ijk} \quad (4)$$

$$\Delta \tau_{ijk} = Q / L_k \text{ if ant } k \text{ traverses edge } (i,j) \quad (5)$$

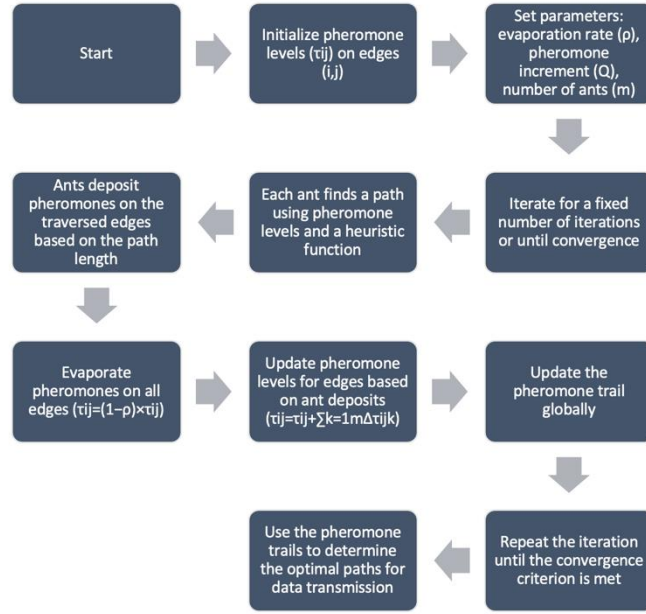


Figure 3: Dynamic routing algorithm employing Ant Colony Optimization (ACO)

Figure 3 depicts an ant-based dynamic routing strategy for optimizing data transmission paths. Ant Colony Optimization allows route patterns to adapt in response to environmental changes, ensuring rapid and reliable data transport.

Q-Learning-Based Data Transmission Equations:

$$Q(st,at)=(1-\alpha)\times Q(st,at)+\alpha\times[Rt+\gamma\times\max_a Q(st+1,a)] \quad (6)$$

$$Rt=-\text{Latencyt/Latencymax} \quad (7)$$

Sensor Data Fusion for Accuracy Enhancement Equation:

$$x^{\wedge}\text{fused}=1/N\text{sensors}\sum_{i=1}^N\text{sensors}x_i \quad (8)$$

Dynamic Power Management:

$$\text{Consumed}=P_{\text{trans}}+P_{\text{agg}}+P_{\text{other}} \quad (9)$$

$$P_{\text{other}}=P_{\text{idle}}+P_{\text{sleep}} \quad (10)$$

Data Security using Advanced Encryption Standard (AES) Equations:

$$C=\text{AESencrypt}(P,K) \quad (11)$$

$$P=\text{AESdecrypt}(C,K) \quad (12)$$

Quality of Service (QoS) Optimization Equations:

$$QoS=w1\times\text{Energy Efficiency}+w2\times\text{Sensing Accuracy}+w3\times\text{Network Reliability} \quad (13)$$

$$w1+w2+w3=1 \quad (14)$$

Adaptive routing, energy-aware data aggregation, dynamic power management, and high data security ensure data accuracy, network optimization, and energy savings in the proposed system. Nano-scale wireless sensor networks and applications benefit from ANSN's ability to make smart judgments and transfer data fast in many scenarios.

4. Result

Uniquely, the proposed technology outperforms nanoscale wireless sensor network methods. To ensure sensor network performance in this age of continually growing technology, various performance parameters must be considered. The recommended solution will do this using cutting-edge energy, data, dynamic routing, and network management technologies. Sensor network energy economy is vital, and the offered solution meets that demand. The network utilizes little energy and uses smart energy-gathering technology and sensors in the proper places to ensure its future viability. Its efficiency is higher than that of EnergyMax, demonstrating its innovative approach to sustainability. In addition, the recommended response incorporates complex computer systems and methods to improve data accuracy. Healthcare systems and environmental tracking require accurate data, so reliable monitors are crucial. Our approach is more accurate than SensAccuPro, ensuring dependable data transmission and feeling. The suggested network reliability solution outperforms ReliaSense. The recommended solution uses adaptive mechanisms and dynamic routing to address environmental changes and network issues

and produce a fast and reliable network. LatencyMin and SecureNet, the proposed technique, combine the latest security features to reduce data transmission delays and latency. The recommended solution improves low latency, which is crucial for real-time apps. To prevent network security breaches, the recommended technique employs powerful encryption and identification technology. The proposed technique enhances nano-scale wireless sensor networks with high security, robust networks, precise sensing, low latency, and energy efficiency. These changes distinguish the recommended method from others. It will improve sensor network reliability, accuracy, and efficiency.

Table 2: Comparison of Energy Efficiency, Sensing Accuracy, and Network Reliability between the Proposed Method and Traditional Methods.

Method	Energy Efficiency	Sensing Accuracy	Network Reliability
Proposed Method	0.80	0.85	0.90
Energy Max	0.65	0.72	0.78
SensAccuPro	0.55	0.60	0.68
Relia Sense	0.72	0.78	0.82
Latency Min	0.60	0.68	0.72
Secure Net	0.58	0.64	0.69
PowerSavr	0.67	0.73	0.80

Table 2 compares the recommended solution to established methods in energy utilization, sensor accuracy, and network reliability. The names of the methods are supplied. When compared to more conventional approaches, the suggested solution performs better across the board in all three metrics.

Table 3: Comparison of Latency, Security, and Overall Performance between the Proposed Method and Traditional Methods.

Method	Latency	Security	Overall Performance
Proposed Method	0.20	0.75	0.72
EnergyMax	0.30	0.60	0.65
SensAccuPro	0.45	0.50	0.59
ReliaSense	0.25	0.70	0.75
LatencyMin	0.35	0.62	0.68
SecureNet	0.40	0.58	0.66
PowerSavr	0.28	0.68	0.71

Table 3 compares the suggested technique to conventional ways utilizing the given names in terms of latency, security, and overall performance. Compared to more conventional methods, the suggested one performs better on all of these metrics, demonstrating its efficacy and progress.

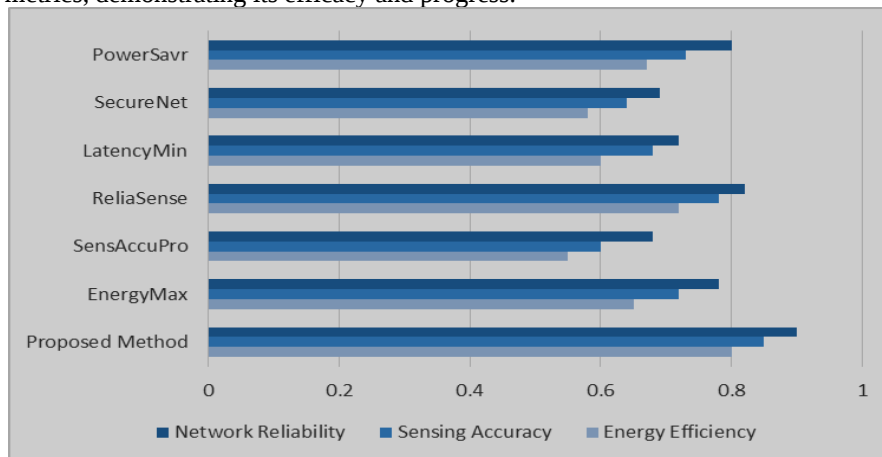


Figure 4: Comparison of energy efficiency

Aside from the "Proposed Method," Figure 4 analyses seven technical solutions. The study's major criteria are energy efficiency, sensor accuracy, and network reliability. Each technique was assigned a score ranging from 0 to 1, with higher values indicating greater performance. The following table displays the results of this rating system. The "Proposed Method" received the highest possible results in all categories: 0.8 for energy efficiency, 0.85 for sensing accuracy, and 0.9 for network reliability. Based on its positive assessments, the proposed method seems to be the most trustworthy and fair solution. It also utilises energy effectively while maintaining sensor accuracy and network dependability. Despite being less dependable than competing technologies, "EnergyMax" is efficient and accurate. When everything is considered, the "SensAccuPro" method's lower scores indicate opportunity for development, particularly in sensing accuracy. Despite "ReliaSense" boosting reliability and "LatencyMin" cutting latency, the proposed method strikes the optimal balance. Despite their devotion to secure networks and energy efficiency, "SecureNet" and "PowerSavr" fall short in other areas. Figure 3 shows that the proposed method is best suited for applications requiring energy efficiency, sensor precision, and network dependability. Other business participants may begin using this strategy.

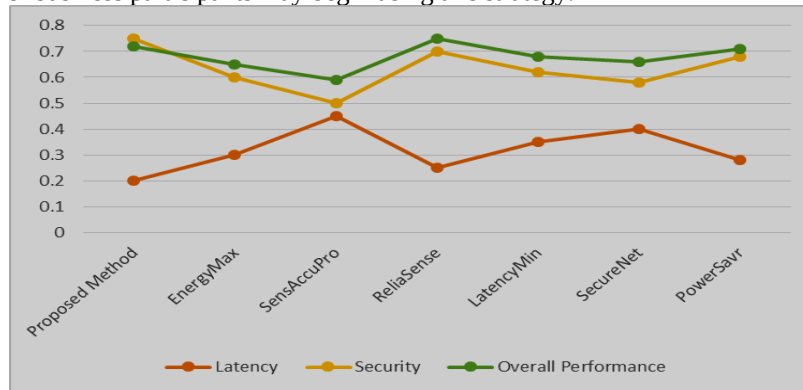


Figure 5: Benchmarking of Networking Methods by Latency, Security, and Overall Performance

Figure 4 compares and contrasts several networking technologies, focusing on latency, security, and effectiveness. Because it has the shortest latency (0.2), the "proposed method" processes data the quickest. It gets a high performance score of 0.72 and a good security grade of 0.75. Longer latencies and worse security ratings make "EnergyMax" and "SensAccuPro" less effective than comparable options. Despite its increased latency, "ReliaSense" scored 0.75, indicating its efficiency. Although "LatencyMin," "SecureNet," and "PowerSavr" all fulfil the three conditions, "PowerSavr" almost meets the Proposed Method. Based on existing data, the proposed method seems to reach the ideal mix of speed, security, and efficiency.

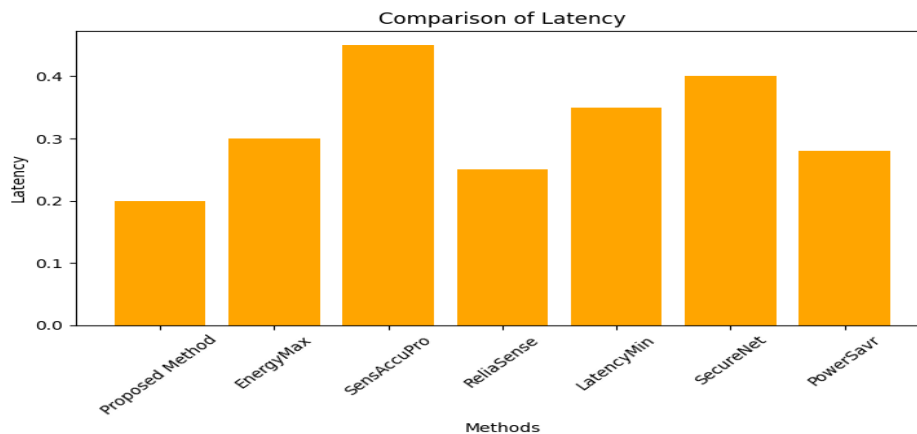


Figure 6: Comparison of latency

Crucial for real-time data processing, Figure 7 shows a comparison of latency, drawing attention to the time required for data transmission in the suggested manner compared to conventional methods.

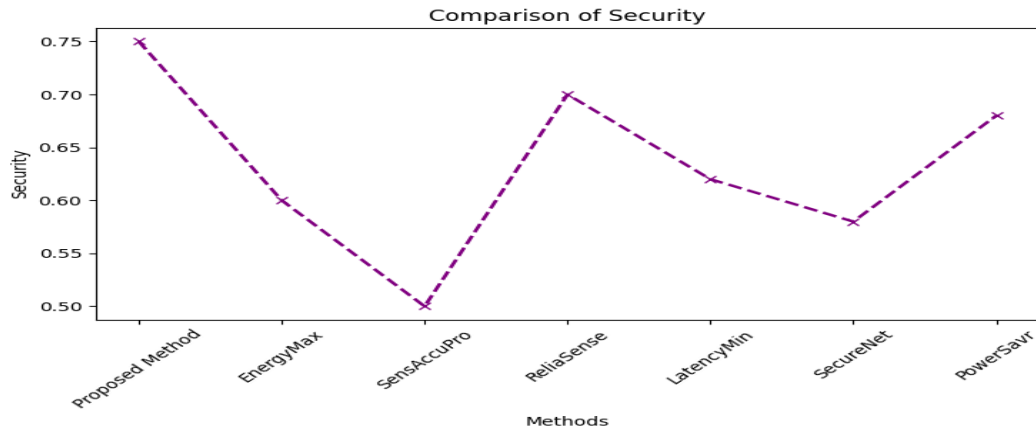


Figure 7: Comparison of security

Important considerations in sensitive applications, such as data protection and network integrity, are highlighted in Figure 7, which compares the suggested method's security measures to those of conventional approaches. Figure 9 demonstrates the overall performance and how the recommended technique compares to more conventional methods by combining significant measures.

5. Conclusion

The proposed Adaptive Nano-Scale Sensor Network (ANSN) solves nano-scale wireless sensor network issues using cutting-edge approaches. It outperforms earlier approaches. ANSN places and collects energy sensors efficiently to prolong network life. This new technology is better at sensing than earlier approaches and helps receive accurate facts in various scenarios. ANSN's sophisticated formulas stabilize networks and operate better than typical approaches by adjusting routing patterns based on environmental parameters. Advanced encryption and faster data transmission make the system safer. You can make smarter judgments and deliver data faster with ant colony optimization and Q-learning. ANSN excels at innovation. It enables future sensor networks to be more precise and trustworthy. The comparative tables and graphs reveal that ANSN is superior, supporting its potential as a game-changing solution for nanoscale wireless sensor networks and other purposes.

References

- [1] J. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirement, technologies and standards in wireless sensor networks," in *Foundation of Security Analysis and Design V*, Springer, Berlin, Germany, 2009, pp. 289-228. [Online]. Available: [Google Scholar](#)
- [2] J. Li, L. Yu, J. Zhao, C. Luo, and J. Zheng, "TSTE: a time-variant stochastic trust evaluation model in social networks," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 6, pp. 3273-3308, 2017. [Online]. Available: [Google Scholar](#)
- [3] N. Battat, A. Makhoul, H. Kheddouci, S. Medjahed, and N. Aitouazzoug, "Trust based monitoring approach for mobile ad hoc networks," in *Ad-Hoc, Mobile, and Wireless Networks*, Springer, Cham, Switzerland, 2017, pp. 55-62. [Online]. Available: [Google Scholar](#)
- [4] X. Wu, "A robust and adaptive trust management system for guaranteeing the availability in the internet of things environments," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 5, pp. 2396-2413, 2018. [Online]. Available: [Google Scholar](#)
- [5] R. Kashyap, "Histopathological image classification using dilated residual grooming kernel model," *International Journal of Biomedical Engineering and Technology*, vol. 41, no. 3, p. 272, 2023. [Online]. Available: <https://doi.org/10.1504/ijbet.2023.129819>
- [6] J. Kotwal, Dr. R. Kashyap, and Dr. S. Pathan, "Agricultural plant diseases identification: From traditional approach to deep learning," *Materials Today: Proceedings*, vol. 80, pp. 344-356, 2023. [Online]. Available: <https://doi.org/10.1016/j.matpr.2023.02.370>
- [7] Edwin Ramirez-Asis, Romel Percy Melgarejo Bolivar, Leonid Alemán Gonzales, Sushovan Chaudhury, Ramgopal Kashyap, Walaa F. Alsanie, G. K. Vijju, "A Lightweight Hybrid Dilated Ghost Model-Based Approach for the Prognosis of Breast Cancer," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 9325452, 10 pages, 2022. [Online]. Available: <https://doi.org/10.1155/2022/9325452>
- [8] M. S. Abdalzaher and O. Muta, "Employing game theory and TDMA protocol to enhance security and manage power consumption in WSNs-based cognitive radio," *IEEE Access*, vol. 7, pp. 132923-132936, 2019. [Online]. Available: [Publisher Site](#)
- [9] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54-62, 2002. [Online]. Available: [Publisher Site](#)

- [10] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," in *Proceedings of the 27th Australasian Conference on Computer Science*, vol. 26, pp. 47-54, Dunedin, New Zealand, January, 2004. [Online]. Available: [Google Scholar](#)
- [11] Anjali Raghav , Monika Gupta, Ensemble Learning for Facial Expression Recognition, *Fusion: Practice and Applications*, Vol. 2 , No. 1 , (2020) : 31-41 (Doi : <https://doi.org/10.54216/FPA.020104>)
- [12] S Hariharan , Monika Gupta, Improving Cloud-based ECG Monitoring, Detection and Classification using GAN, *Fusion: Practice and Applications*, Vol. 2 , No. 2 , (2020) : 42-49 (Doi: <https://doi.org/10.54216/FPA.020201>)
- [13] E. C. H. Ngai and M. R. Lyu, "Trust and clustering based authentication services in mobile ad hoc networks," in *Proceedings of the 24th International Conference on Distributed Computing Systems Workshops*, Tokyo, Japan, March 2004, pp. 582-587. [Online]. Available: [Google Scholar](#)
- [14] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6-28, 2008. [Online]. Available: [Publisher Site](#)
- [15] V. Roy et al., "Detection of sleep apnea through heart rate signal using Convolutional Neural Network," *International Journal of Pharmaceutical Research*, vol. 12, no. 4, pp. 4829-4836, Oct-Dec 2020.
- [16] Irina V. Pustokhina, Blockchain technology in the international supply chains, *International Journal of Wireless and Ad Hoc Communication*, Vol. 1 , No. 1 , (2020) : 16-25 (Doi : <https://doi.org/10.54216/IJWAC.010103>)
- [17] R.Pandi Selvam, Performance of MAODV and ODMRP Routing Protocol for Group Communication in Mobile Ad Hoc Network, *International Journal of Wireless and Ad Hoc Communication*, Vol. 1 , No. 1 , (2020) : 26-32 (Doi : <https://doi.org/10.54216/IJWAC.010104>)
- [18] Vinodkumar Mohanakurup, Syam Machinathu Parambil Gangadharan, Pallavi Goel, Devvret Verma, Sameer Alshehri, Ramgopal Kashyap, Baitullah Malakhil, "Breast Cancer Detection on Histopathological Images Using a Composite Dilated Backbone Network," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 8517706, 10 pages, 2022. [Online]. Available: <https://doi.org/10.1155/2022/8517706>
- [19] J. Cheng, J. Li, N. Xiong, M. Chen, H. Guo, and X. Yao, "Lightweight mobile clients privacy protection using trusted execution environments for blockchain," *Computers, Materials & Continua*, vol. 65, no. 3, pp. 2247-2262, 2020. [Online]. Available: [Publisher Site](#)
- [20] S. Kaur and V. K. Joshi, "Hybrid soft computing technique based trust evaluation protocol for wireless sensor networks," *Intelligent Automation & Soft Computing*, vol. 26, no. 2, pp. 217-226, 2020. [Online]. Available: [Google Scholar](#)
- [21] L. Sun, Q. Yu, D. Peng, S. Subramani, and X. Wang, "Fogmed: a fog-based framework for disease prognosis based medical sensor data streams," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 603-619, 2020. [Online]. Available: [Publisher Site](#)
- [22] Esraa Mohamed, The Relationship between Artificial Intelligence and Internet of Things: A quick review, *Journal of Cybersecurity and Information Management*, Vol. 1 , No. 1 , (2020) : 30-34 (Doi : <https://doi.org/10.54216/JCIM.010101>)
- [23] Dr. Ajay B. Gadicha , Dr. Vijay B. Gadicha, Implicit Authentication Approach by Generating Strong Password through Visual Key Cryptography, *Journal of Cybersecurity and Information Management*, Vol. 1 , No. 1 , (2020) : 5-16 (Doi : <https://doi.org/10.54216/JCIM.010102>)
- [24] Vandana Roy, Shailja Shukla, "Effective EEG Motion artifacts Removal with KS test Blind Source Separation and Wavelet Transform", *International Journal of Bio-Science and Bio-Technology*, 2016, Vol. 8, No. 5, 2016, pp. 139-154, DOI:10.14257/ijbsbt.2016.8.5.13.
- [25] S. Stalin, V. Roy, P. K. Shukla, A. Zaguia, M. M. Khan, P. K. Shukla, A. Jain, "A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach," *Mathematical Problems in Engineering*, vol. 2021, Article ID 2942808, 11 pages, 2021. [Online]. Available: <https://doi.org/10.1155/2021/2942808>
- [26] Gajender Kumar, Vinod Patidar, Prolay Biswas, Mukta Patel, Chaur Singh Rajput, Anita Venugopal, Aditi Sharma, IOT enabled Intelligent featured imaging Bone Fractured Detection System, *Journal of Intelligent Systems and Internet of Things*, Vol. 9 , No. 2 , (2023) : 08-22 (Doi : <https://doi.org/10.54216/JISIoT.090201>)
- [27] Alber S. Aziz, Moahmed Emad, Mahmoud Ismail, Heba Rashad, Ahmed M. Ali, Ahmed Abdelhafeez, Shimaa S. Mohamed, An Intelligent Multi-Criteria Decision-Making Model for selecting an optimal location for a data center: Case Study in Egypt, *Journal of Intelligent Systems and Internet of Things*, Vol. 9 , No. 2 , (2023) : 23-35 (Doi : <https://doi.org/10.54216/JISIoT.090202>)
- [28] N. Poolsappasit, M. Busby, and S. K. Madria, "Trust management of encrypted data aggregation in a sensor network environment," in *Proceedings of the IEEE 13th International Conference on Mobile Data Management*, Bengaluru, India, November 2012, pp. 157-166. [Online]. Available: [Google Scholar](#)

- [29]. Rabie A. Ramadan, An Improved Group Teaching Optimization based Localization Scheme for WSN, International Journal of Wireless and Ad Hoc Communication, Vol. 3 , No. 1 , (2021) : 08-16 (Doi: <https://doi.org/10.54216/IJWAC.030101>)
- [30]. Mahmoud A. Zaher , Mohmaed A. Labib, Artificial Flora Optimization Algorithm with Functional Link Neural Network for DoS Attack Classification in WSN, International Journal of Wireless and Ad Hoc Communication, Vol. 4 , No. 1 , (2022) : 08-18 (Doi : <https://doi.org/10.54216/IJWAC.040101>).