

An Optimized Clustering Approach for Enhancing Security and Prolonging Network Lifetime in Wireless Sensor Networks

Divya Srivastava, Nitin Jain, Manish Kumar

Electronics and Communication Department, BBD university, Lucknow, India^{1,2}

Electronics and Communication Department, SUAS, Indore, India

divya.div1912@gmail.com

Abstract: Wireless sensor networks (WSNs) are important in various industries due to their scalability, low maintenance, and self- IoT-connected tiny sensor nodes capture environmental conditions in these networks. Ad hoc communication topology for autonomous operations is established by these nodes. However, sensor nodes' limited energy, data storage, transmission bandwidth, and processing capacity present issues. Battery-powered nodes reduce network efficiency, therefore these limits must be addressed. Network speed, energy balance, and data integrity persist despite research. This is exacerbated by sensor node security flaws, especially in dynamic networks. Protecting these vulnerabilities against data compromise is critical. This work creates a safe, energy-efficient WSN routing system using heuristics. Protocol proposes two methods: First, it uses PSO-based heuristic analysis to provide a smart, adaptable learning mechanism for trustworthy routing. Second, its lightweight, computationally simple security structure safeguards data communications from dangerous attacks. Network disconnections and link failures are reduced via traffic exploration to optimise route maintenance. Simulations reveal that PSO-based protocols outperform prior approaches in dynamic networks. It increases network speed by 18%, packet drop by 42%, latency by 26%, energy use by 36%, inappropriate route minimisation by 38%, network overhead by 44%, and compute overhead by 43%. The protocol boosts WSN performance and addresses energy and security issues.

Keywords: Wireless sensor networks, heuristic analysis, energy efficiency, artificial intelligence, and data privacy.

1. Introduction:

Because of its ability to watch and collect physical data, Wireless Sensor Networks (WSNs) are being thoroughly investigated in a variety of applications, such as military operations, healthcare systems, smart infrastructures, and agriculture [1]–[3]. The sensor nodes that make up these networks can be uniformly or randomly distributed to collect data on a regular basis or in response to particular events. Data is transmitted to a base station (BS) so that end users can access it through wireless broadband channels on the Internet [4], [5]. WSNs are useful in many academic and industrial domains, but

their functionality is limited by a number of issues. These include restrictions on battery life, memory, computing power, and transmission capacity [6], [7]. For many applications, increasing energy efficiency while guaranteeing reliable data delivery continues to be a crucial task.

The self-configured nature, ad hoc operation, and simplicity of deployment and maintenance of WSN infrastructure distinguish it from conventional networks. Multi-hop data transmission is frequently used to relay data to the base station across wide network locations. Clustering sensor nodes into discrete zones has been the subject of recent study, where a cluster head is assigned for a certain amount of time to gather and transmit data from its members to the BS [8]–[10].

Research on scalability, the network, and efficient data routing is becoming more and more crucial as WSNs get bigger and more sensor nodes join the network. In general, there are two types of routing protocols for data distribution: static and dynamic techniques [11]–[13]. Because static routing has a reduced processing overhead and requires manual routing table maintenance by gateway nodes and routers, it is better suited for smaller networks. On the other hand, dynamic routing is better for high-density networks since it automatically updates routing tables in response to events or changes in the network. Dynamic systems, on the other hand, need a lot of processing and are more vulnerable to problems like transmission unreliability and channel interference, which are more common in wireless networks than in wired ones.

Many methods have been inspired by the development of wireless network routing technologies like DSR and AODV [14]–[16]. However, the majority are unable to effectively address the difficulties presented by the dynamic behaviour of WSNs and the low-power characteristics of sensor nodes. In constraint-oriented networks, important issues including energy efficiency, throughput, and network scalability continue to be significant research difficulties.

The seamless exchange of physical information via smart devices, RFID technologies, and IoT-enabled sensors is made possible by the integration of IoT with WSNs, which adds new dimensions in addition to these difficulties [17]–[19]. For analysis and decision-making, these sensors send the BS the data they have acquired. However, sensor nodes are more susceptible to security risks due to their restricted capabilities, particularly with regard to battery life, memory, and computational power. Unauthorised access, data breaches, and

compromised network confidentiality and integrity are all made more likely by these vulnerabilities. While many current solutions concentrate on improving energy economy and data delivery, they frequently ignore the crucial component of sensor data security, leaving networks vulnerable to possible assaults. IoT-based WSNs need a routing solution that strikes a balance between energy efficiency and strong security to handle these issues and shield network data from malevolent assaults, unauthorised access, and manipulation. [20], [21].

In order to maximise WSN performance, this study suggests a safe and energy-efficient heuristic routing protocol called SEHR that incorporates artificial intelligence approaches. SEHR, which was created especially for contexts with limited resources, emphasises accomplishment. To find the best routing path reliability, energy efficiency, and secure data transfer, the protocol uses an optimization-based beam metaheuristic algorithm [22]. Intelligent routing decisions are made using a PSO-based method that takes into account variables including hop count, residual energy, and connection integrity. The artificial intelligence-based beam-based heuristic technique improves routing results by reducing processing overhead and sensor node memory needs.

To guarantee safe and verified data routing, the SEHR protocol also uses a cryptographic counter mode (CTR) approach. This technique improves security and authenticity by encrypting data packets in a sequential manner, with each packet depending on the encryption of the one before it. A route maintenance technique is incorporated to dynamically identify and isolate malicious nodes throughout the data security stage, further fortifying the protocol. Effective load distribution and mitigation of problems like network disconnections are achieved through alerts for energy levels and traffic analysis between the BS and its clusters.

The suggested SEHR protocol greatly improves network performance for low-powered sensor nodes across a number of parameters as compared to cutting-edge techniques. It tackles the urgent issues of scalability, throughput, and data security in WSNs while guaranteeing safe and energy-efficient operation.

2. Related Work:

Many protocols for Wireless Sensor Networks (WSNs) have been developed in recent years, with a focus on applications like healthcare, smart cities, military systems, and smart transportation [24]–[27]. However, because sensor nodes have limited resources, there are numerous challenges, such as decreased network performance and the requirement for safe, energy-efficient routing.

Faster data path establishment is made possible by proactive routing protocols, which share information with neighbours to update node tables on a regular basis. However, this method causes network congestion and significant control packet overhead. On the other hand, when a data packet is received, reactive (on-demand) protocols—which are frequently employed in wireless networks—determine the next hop depending on neighbour information. Compared to proactive approaches, they lower network overhead even while they

cause packet forwarding delays. An Adaptive Competition-Based Clustering Approach (ACCA) for WSN was proposed by the authors in [28], taking into account factors including remaining energy, node centrality, and cluster head separation for cluster head selection. This approach uses multi-hop data transfer and balances cluster sizes by taking into consideration the distance between cluster heads. However, because of data security risks, it is not appropriate for large-scale deployments and lacks connection evaluation during cluster head selection. Five parameters were used to choose cluster heads and guarantee uniform distribution in [29], an energy-efficient clustering method based on fuzzy logic. Even while performance is better, this approach uses more energy and produces a lot of control packets, which leaves it open to malicious traffic. In order to guarantee secure connection and cut down on superfluous traffic, a node-to-node transmission protocol with fog and cloud layers was proposed in [30] for next-generation smart city networks. Nevertheless, the method did not assess energy efficiency and network overhead. To reduce jamming attacks and enhance data transmission, a safe routing system for IoT-based cognitive radio networks was developed in [31]. However, it only used the packet delivery ratio to assess performance, ignoring important network parameters. Similar to this, the SecTrust-RPL protocol in [32] improved routing security against network attacks, but poor routing choices jeopardised data transmission. A cooperative communication-based security system enhanced cyberattack resilience and data reliability in [33]. Notwithstanding these advantages, it performed poorly in routing and was most appropriate for small sensor nodes.

The Predictive Efficient Energy Consumption Reclaim (PEECR) technique was proposed by the authors in [34]. It uses swarm optimisation for routing based on residual energy, clustering distance, and node degree. Despite its great performance, its security was compromised by its large control message overhead and absence of data integrity protections. In [35], a protocol based on particle swarm optimisation sought to increase network lifetime by lowering the energy consumption of gateway nodes. Although efficient, it disregarded connection integrity and security when making routing choices.

An enhanced hierarchical clustering technique utilising fuzzy inference systems was introduced in [36] for mobile sensor networks, resulting in increased cluster stability and network lifetime. However, the method has trouble with security threats and real-time node mobility. By choosing cluster heads based on closeness and residual energy, a fuzzy logic-based clustering method (CAFL) in [37] increased network longevity. However, it lacked effective routing and secure transfers. Similar to this, the Enhanced Clustering Hierarchy (ECH) technique in [38] decreased redundant data and increased energy efficiency, but it was unable to handle network attacks and sensor node limits. [39] developed a heuristic data transmission strategy utilising a double-ring mediator to overcome hotspot problems in mobile sink networks. By using residual energy and transmission distance heuristics, this decreased the frequency of location

updates and increased energy efficiency. In [40], an energy-efficient routing method used the Temporary Energy Mapping Algorithm (TEMA) for route maintenance and the African Buffalo-based Two-tier Data Dissemination (AB-TTDD) strategy. Although these techniques improved packet delivery and power consumption, they lacked defences against malevolent attacks and frequently necessitated route rediscoveries since wireless link dynamics were disregarded

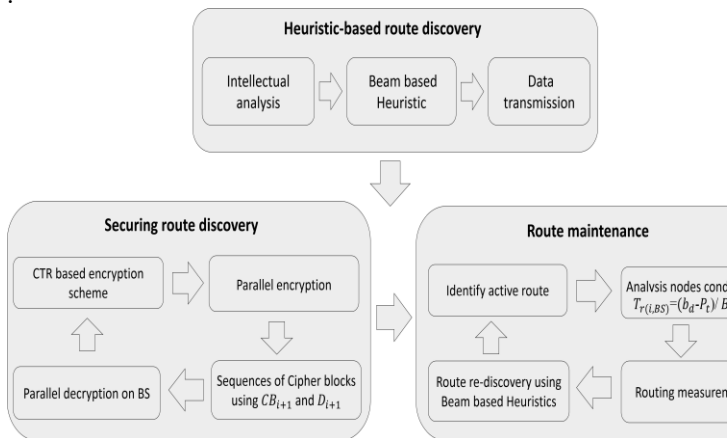


Fig. 1: The design of architecture of the PSO based protocol

3. Result and Discussion:

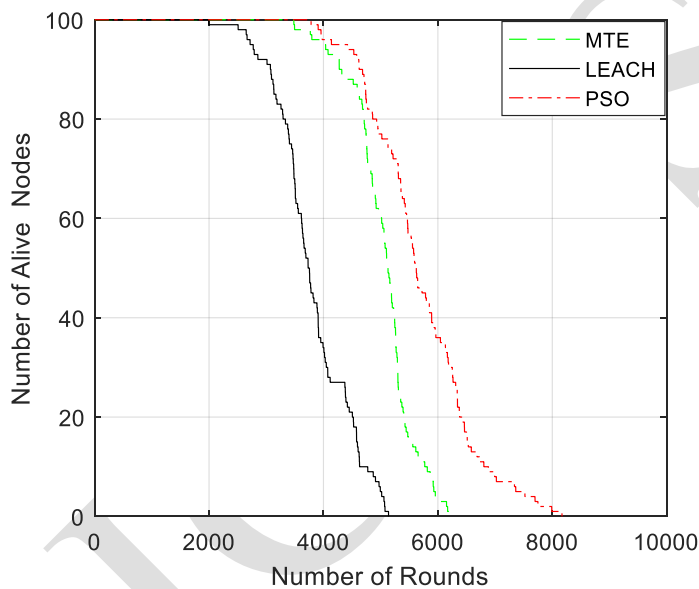


Fig. 2: Number of alive node and Number of rounds

Extensive simulations were carried out using the MATLAB software to evaluate the efficacy of the proposed method and its effect on the total network energy. To achieve rigorous analysis, several random node placements were used in these simulations. Table 1 provides a summary of the simulation settings used in this investigation. A packet size of $L=2000$ bits was selected, and 50 sensor nodes were dispersed at random

throughout a 100 m x 100 m network space. In the suggested method, the likelihood of each node becoming a cluster head was set at 0.05, and the base station (BS) was positioned strategically at coordinates $(x=50 \text{ m}, y=-100 \text{ m})$. Since it allows for quick monitoring of the algorithm's impacts on energy consumption, the energy level of 0.5 J was first set for each sensor node. This value is frequently used in the literature. The suggested method was compared with the Minimum Transmission Energy (MTE) protocol using critical performance metrics such as First Node Dies (FND), Half of Nodes Alive (HNA), Last Node Dies (LND), and Energy Depletion Rate (EDR). The measures' outcomes and compares the suggested technique to LEACH, MTE, and the basis paper methodology. These performance measures were used to assess the suggested method's technical capabilities. The number of active nodes per round for the basic paper and the recommended method is shown in Figure 3. By allowing for more rounds of operation than the baseline method, the proposed method greatly extends the stability period, which is defined as the time interval from the network's initialisation until the death of the first sensor node. This demonstrates the improved network longevity and energy efficiency attained by putting the suggested approach into practice.

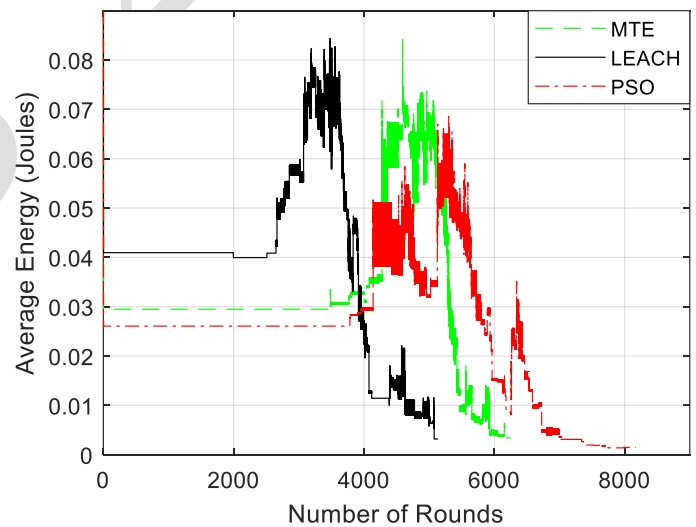


Fig. 3: Average energy consumption and Number of rounds

A comparison of the three methods' combined average energy consumption each round is shown in Figure 3. With the multi-hop cluster-based routing approach, the network's lifespan is greatly increased, outperforming conventional base paper protocols. By utilising the PSO (Particle Swarm Optimisation) algorithm inside each cluster, the suggested approach optimises data routing. This method primarily uses free-space propagation and carefully considers the distance between nodes. Traditional multi-path propagation is replaced with reduced inter-node distances, which act as the connection cost parameter. The energy efficiency of the network as a whole is

effectively increased by this modification to the propagation model.

4. Conclusion:

In order to optimise routing techniques and cleverly lessen the impact of malicious nodes, this paper proposes a protocol for secure and energy-aware heuristic routing (SEHR) for WSN. The protocol's main focus is on crucial elements like energy consumption, secure data transfer, and route maintenance to guarantee dependable and trustworthy transmissions. By taking into account factors including residual energy, hop count to the base station (BS), and connection integrity, the SEHR protocol's metaheuristic optimisation function enhances network performance. The possibility of network disconnections is decreased and route maintenance is further improved by traffic analysis close to the base station. The counter mode encryption method, which is known for its randomness, simplicity, and lightweight construction, is used by the SEHR protocol to secure data. Parameters like node count and data generation rates are used in simulation-based evaluations. In order to improve the network's intelligence and resilience, future developments will incorporate machine learning techniques into the SEHR protocol in a lightweight manner. Furthermore, energy efficiency and routing performance can be further enhanced by addressing asynchronous duty cycles among sensor nodes.

References

- [1] O. I. Khalaf and B. M. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Periodicals Eng. Natural Sci.*, vol. 7, no. 3, pp. 1096–1101, 2019.
- [2] B. Bhushan and G. Sahoo, "Routing protocols in wireless sensor networks," in *Computational Intelligence in Sensor Networks*. Berlin, Germany: Springer, 2019, pp. 215–248.
- [3] X. Liu, T. Qiu, and T. Wang, "Load-balanced data dissemination for wireless sensor networks: A nature-inspired approach," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9256–9265, Dec. 2019.
- [4] V. Chetlapalli, K. S. S. Iyer, H. Agrawal, and S. Patil, "A new approach to modeling time dependent problems in wireless broadband networks," in *Proc. ACM Workshop Distrib. Inf. Process. Wireless Netw. (DIPWN)*, 2017, pp. 1–6.
- [5] B. P. Rimal, M. Maier, and M. Satyanarayanan, "Experimental testbed for edge computing in fiber-wireless broadband access networks," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 160–167, Aug. 2018.
- [6] J.-A. Fernandez-Prieto, J. Caçada-Bago, and M.-A. Gadeo-Martos, "Wireless acoustic sensor nodes for noise monitoring in the city of linares (JaØn)," *Sensors*, vol. 20, no. 1, p. 124, Dec. 2019.
- [7] S. Dutt, S. Agrawal, and R. Vig, "Cluster-head restricted energy efficient protocol (CREEP) for routing in heterogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 100, no. 4, pp. 1477–1497, 2018.
- [8] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trustbased secure clustering in WSN-based intelligent transportation systems," *Comput. Netw.*, vol. 146, pp. 151–158, Dec. 2018.
- [9] S. K. Singh, P. Kumar, and J. P. Singh, "An energy efficient protocol to mitigate hot spot problem using unequal clustering in WSN," *Wireless Pers. Commun.*, vol. 101, no. 2, pp. 799–827, Jul. 2018.
- [10] S. Kumar, "Compartmental modeling of opportunistic signals for energy efficient optimal clustering in WSN," *IEEE Commun. Lett.*, vol. 22, no. 1, pp. 173–176, Jan. 2018.
- [11] B. K. Gupta, S. Patnaik, M. K. Mallick, and A. K. Nayak, "Dynamic routing algorithm in wireless mesh network," *Int. J. Grid Utility Comput.*, vol. 8, no. 1, pp. 53–60, 2017.
- [12] E. Akin and T. Korkmaz, "Comparison of routing algorithms with static and dynamic link cost in SDN," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–8.
- [13] T. Nebbou, M. Lehsaini, and H. Fouchal, "Partial backwards routing protocol for VANETs," *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100162.
- [14] M. Rath, B. K. Pattanayak, and B. Pati, "Energetic routing protocol design for real-time transmission in mobile ad hoc network," in *Computing and Network Sustainability*. Singapore: Springer, 2017, pp. 187–199.
- [15] W. B. Gong, X. L. Yang, M. Zhang, and K. Long, "Multi-path routing protocol based on adaptation mechanism of cell in ad hoc networks," *J. Commun.*, vol. 35, no. 6, pp. 56–63, 2019.
- [16] S. Salari-Moghaddam, H. Taheri, and A. Karimi, "Trust based routing algorithm to improve quality of service in DSR protocol," *Wireless Pers. Commun.*, vol. 109, no. 1, pp. 1–16, Nov. 2019.
- [17] K. Haseeb, N. Islam, T. Saba, A. Rehman, and Z. Mehmood, "LSDAR: A light-weight structure based data aggregation routing protocol with secure Internet of Things integrated next-generation sensor networks," *Sustain. Cities Soc.*, vol. 54, Mar. 2020, Art. no. 101995.
- [18] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards Internet of Things," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–6.
- [19] I. Ud Din, M. Guizani, B.-S. Kim, S. Hassan, and M. Khurram Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019.
- [20] S. Pirbhulal, H. Zhang, M. E. Alahi, H. Ghayvat, S. Mukhopadhyay, Y.-T. Zhang, and W. Wu, "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, no. 12, p. 69, Dec. 2016.
- [21] J. Qian, H. Xu, and P. Li, "A novel secure architecture for the Internet of Things," in *Proc. Int. Conf. Intell. Netw. Collaborative Syst. (INCoS)*, Sep. 2016, pp. 311–314.
- [22] R. Bisiani, "Beam search," in *Encyclopedia of Artificial Intelligence*, S. Shapiro, Ed. Hoboken, NJ, USA: Wiley, 1987, pp. 56–58.

International Conference on Intelligent Technologies & Science - 2025 (ICITS-2025)

- [23] H. Lipmaa, P. Rogaway, and D. Wagner, "Comments to NIST concerning AES modes of operations: CTR-mode encryption," in *Proc. Symmetric Key Block Cipher Modes Operation Workshop*, Baltimore, MD, USA, 2000.
- [24] I. A. Ridhawi, M. Aloqaily, and A. Boukerche, "Comparing fog solutions for energy efficiency in wireless networks: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 80–86, Dec. 2019.
- [25] I. Jawhar, N. Mohamed, and J. Al-Jaroodi, "Networking architectures and protocols for smart city systems," *J. Internet Services Appl.*, vol. 9, no. 1, p. 26, Dec. 2018.
- [26] A. Onasanya, S. Lakkis, and M. Elshakankiri, "Implementing IoT/WSN based smart saskatchewan healthcare system," *Wireless Netw.*, vol. 25, no. 7, pp. 3999–4020, Oct. 2019.
- [27] D. C. Huang, Y. Y. Chu, Y. K. Tzeng, and Y. Y. Chen, "Secure routing for WSN-based tactical-level intelligent transportation systems," *J. Internet Technol.*, vol. 20, no. 4, pp. 1013–1026, 2019.
- [28] M. Afsar, M.-H. Tayarani-N., and M. Aziz, "An adaptive competitionbased clustering approach for wireless sensor networks," *Telecommun. Syst.*, vol. 61, no. 1, pp. 181–204, Jan. 2016.
- [29] A. Hamzah, M. Shurman, O. Al-Jarrah, and E. Taqieddin, "Energyefficient Fuzzy-Logic-Based clustering technique for hierarchical routing protocols in wireless sensor networks," *Sensors*, vol. 19, no. 3, p. 561, Jan. 2019.
- [30] I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh, and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities," *Sustain. Cities Soc.*, vol. 56, May 2020, Art. no. 102080.
- [31] H. Bany Salameh, R. Derbas, M. Aloqaily, and A. Boukerche, "Secure routing in multi-hop IoT-based cognitive radio networks under jamming attacks," in *Proc. 22nd Int. ACM Conf. Model., Anal. Simul. Wireless Mobile Syst. (MSWIM)*, 2019, pp. 323–327.
- [32] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019.
- [33] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "A novel security protocol for wireless sensor networks with cooperative communication," *Computers*, vol. 9, no. 1, p. 4, Jan. 2020.
- [34] D.-G. Zhang, H.-L. Niu, and S. Liu, "Novel PEECR-based clustering routing approach," *Soft Comput.*, vol. 21, no. 24, pp. 7313–7323, Dec. 2017.
- [35] D. R. Edla, M. C. Kongara, and R. Cheruku, "A PSO based routing with novel fitness function for improving lifetime of WSNs," *Wireless Pers. Commun.*, vol. 104, no. 1, pp. 73–89, Jan. 2019.
- [36] J.-S. Lee and C.-L. Teng, "An enhanced hierarchical clustering approach for mobile sensor networks using fuzzy inference systems," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 1095–1103, Aug. 2017.
- [37] A. H. El and A. Najid, "Fuzzy logic based clustering algorithm for wireless sensor networks," in *Sensor Technology: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2020, pp. 351–371.
- [38] H. El Alami and A. Najid, "ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks," *IEEE Access*, vol. 7, pp. 107142–107153, 2019.
- [39] H. Kuhlani, X. Wang, A. Hawbani, and O. Busaileh, "Heuristic data dissemination for mobile sink networks," *Wireless Netw.*, vol. 26, no. 1, pp. 479–493, Jan. 2020.
- [40] G. S. Binu and B. Shajimohan, "A novel heuristic based energy efficient routing strategy in wireless sensor network," *Peer-Peer Netw. Appl.*, 2020.
- [41] H. Lipmaa, P. Rogaway, and D. Wagner, "CTR-mode encryption," in *Proc. 1st NIST Workshop Modes Operation*, 2000, pp. 1–4.
- [42] W. Koehrsen. (2019). *The Poisson Distribution and Poisson Process Explained*. [Online]. Available: <https://towardsdatascience.com/the-poisson-distribution-and-poisson-process-explained-4e2cb17d459>
- [43] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2000, pp. 1–10.