International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

Review on Fuzzy-ACO Hybrid Routing Framework for Resilient AODV in IoT-Enabled WSN with Link Interference

Anusai Mathur, Professor Amit Thakur
School Of Engineering and Technology, Vikram University, Ujjain University in Ujjain, Madhya Pradesh

ABSTRACT

Researchers and industry professionals are highly interested in Wireless Sensor Networks (WSNs) due to their importance in utilizing low-cost, low-power microelements, such as radios, computers, and sensors, which are often integrated onto a single chip. Recently, the integration of the Internet of Things (IoT) with WSNs has been extensively explored. Effective routing techniques are crucial for optimizing power usage, ensuring Quality of Service (QoS), and maintaining network reliability in IoT-enabled WSNs. This work presents an enhanced energy-aware navigation system that employs the Quantum Firefly Optimization (QFO) method and Neuro-Fuzzy Clustering for IoT-enabled WSNs. The Neuro-Fuzzy Clustering method extends the system's lifetime by automatically grouping sensor nodes into energy-efficient clusters. The QFO method is used to determine the optimal routing paths by considering factors such as energy consumption, QoS, and trust metrics. By incorporating these advanced methodologies, the proposed solution outperforms existing approaches in terms of energy efficiency, routing accuracy, and overall network stability. Simulation results demonstrate that this novel approach has the potential to significantly improve current routing protocols and expand the capabilities of IoT-enabled WSNs. Additionally, to enhance efficiency in mobile computing environments, the security of the intrusion detection system was strengthened through the use of deep learning techniques.

Keywords: Energy Efficiency; Neuro-Fuzzy Clustering; Quantum Firefly Optimization; Routing Algorithms; Wireless Sensor Networks; Quality of Service; Intenet of Things

I. INTRODUCTION

The advancements in communication protocols, ubiquitous computing, application-specific designs have given a nativity to the extension of wireless technology in the form of the Internet of things (IoT) [1]. The advancement in wireless technology first began in 1880 in the form of photophone, electric wireless technology like radio waves. Gradually, wireless technology started making use of microwaves and optical fibers in the 20th century [2]. The major advancement was the introduction of data communication which gave rise to the invention of cellular data service, satellite communication, and wireless sensor networks. Wireless sensor network (WSN) is one of the prominent technologies in wireless communications which has its major impact on real-world applications [3]. WSN came into existence in the early 1950s and was used mainly in surveillance applications in the US military. The WSN is a self-organized group of interconnected sensor devices or nodes which gather information from an area of interest and forward the processed information to a central base station [4].

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

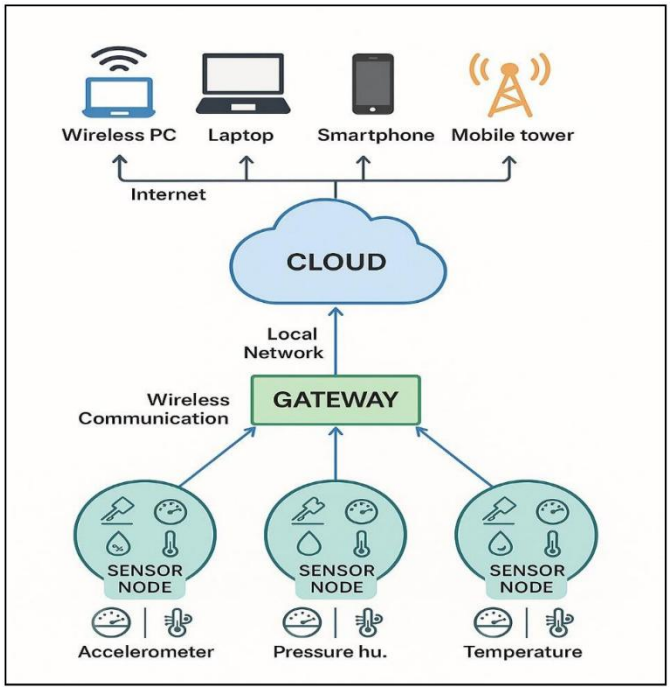

Fig.1. IOT and WSN Gateway.

II. WSN CLUSTERS AND SENSORS

A rapidly emerging combination of technologies known as the "Internet of Things" enables everyday things to collect, process, and exchange data across networks with digital intelligence. IoT, which links the physical and digital worlds, has the potential to enhance environmental perception and proactive decision-making without human intervention. IoT is an interconnected network of machines, electronic and physical items in our environment [1][2]. Wireless sensor networks (WSNs) and cloud compu-ting have been developed quickly and have a wide range of applications, turning the Internet of Things (IoT) from a theoretical notion into a practical reality [3][4]. Wi-Fi is used by IoT to link home appliances to the internet so that they may be managed and controlled remotely. Clusters, sensors, and actuators used in WSN technology to sense and gather data from various smart home components, then send it to a gateway [5]. This study consists of number of sensor nodes forming a Wireless sensor Network with each sensor node was represented by ZigBee end device. The data had been collected by these sensors to be sent the data to the controller. ZigBee served for low cost and low power Wireless sensor network. In this study, ZigBee coordinator performed the controller that sent the data to the gateway so that it could be monitored and controlled by the user. A number of jammers (jamming attacks) had interfered with the normal operation of the network which caused the degradation of the network efficiency. This work aim is to improve IoT based WSN performance degradation because of the Jammers in number of video and file transfer of data applications. The improvement was done using AD-HOC routing protocols which evaluates the best communication pathways for the network data transmission between nodes of the network using soft-ware and routing algorithms in terms of (delay, throughput and data dropped).

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

III. IOT-WSN

Due to the advancement of IoT technology which enable the communication be-tween billions of items, applications, data and people. Since most IoT devices com-municate wirelessly with one another and/or the base station (BS) [2][3]. The WSN serves as a bridge to the Internet of Things. A wireless sensor network is a collection of sensor nodes with a restricted power source and limited computing and transmission capabilities. It is simpler to monitor the challenging environments that are difficult to monitor normally because sensor nodes perceive, analyze, and transmit the observed data to the destination. Routing algorithms can assist to preserve resources and prolong the life of a node by making intelligent decisions based on a realistic lifespan prediction. [4][5]. IoT and WSN are going toward edge technologies. IoT-based Wireless sensor net-works include a wide range of considerations, including communication delay, through-put, security, cost and power consumption. Low-cost sensor nodes for transmission, data collection and remote monitoring are being performed with the rapid rise of IoT-based WSNs [6][7]. Due to an IEEE 802.15.4 standard, the maximum WSN-IoT data rate for end nodes is just 250 kbps. In WSN-IoT, the gateway is connected to the main power source. The cloud server receives the sensor data from the IoT device so that the user could manage and control the program using a desktop PC, laptop, or a mobile device from the IoT cloud. Currently, several well-known cloud service providers offer free with restricted sensor data storage in their cloud storage [8] [9].

IV. AD-HOC ROUTING PROTOCOLS

Evaluates the best communication pathways for the network data transmission be-tween nodes of the network using software and routing algorithms [2].These protocols can be further divided into reactive (on demand), proactive (table driven), and hybrid approaches [3]. Optimized link state routing protocol (OLSR) [4], DV(distance-vec-tor) [2] and Destination Sequenced Distance Vector (DSDV) [25] protocols are the examples of Proactive protocol. Ad Hoc On-Demand Distance Vector (AODV), Dy-namic Source Routing (DSR) [5], and Temporally Ordered Routing Algorithm (TORA) [6] are examples of on-demand routing protocols. ZRP [6] is an example of hybrid routing protocols. ZigBee and IEEE 802.15.4 are two of the most widely utilized protocols for WSN. Among the numerous advantages of ZigBee technology are its ability to conserve bat-tery power, its ability to handle a large number of nodes in a network, and its ability to communicate over long distances. As a result, expanding the network is simple, and it offers high levels of security for its users [7].

V. LOCALIZATION

The localization challenge is very well answered by the use of optimization approaches like PSO, firefly optimization, etc. Still, there is a need to answer some of the issues arising from this challenge for instance the attacks which occur in a sensor network need to be localized in advance by the beacon nodes or by some efficient approach. Also, it is required to reduce the time complexity of the algorithm because as we begin to use a hybrid algorithm to solve any issue, its time complexity enhances. Coverage In the random deployment scenario, the challenge of assigning minimum sensors to cover the whole area of interest is confronting in the way of a successful deployment strategy. The coverage hole caused due to random

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

localization is very hard to predict, so this problem needs to be explored. The 3-D coverage scenario with minimum complexity of computation is also a domain that needs further research.

VI. ANOMALY DETECTION

In the wireless network detecting anomalies is a major challenge that is addressed by many researchers. Some algorithm guarantees the accuracy with less FPR but the complexity goes on increasing. The intrusion creates delay and drops the average throughput of a network. Furthermore, this challenge needs to be answered in the case of WSN assisted IoT networks with high efficiency. Anomaly at the data level is much more critical than at the node level. Once the anomaly is detected, the system must be capable of correcting that anomaly/fault to improve the network's fidelity.

QOS OPTIMIZATION

It is another important aspect of WSN assisted IoT networks. For distinct applications, separate QOS standards are needed which is quite challenging. The cross-layer optimization protocols may be the best means to make the QOS parameters efficient and reliable. For instance, to maintain the synchronization between MAC and the physical layer, there is a need to adjust suitable duty cycles. The development of selfcharging-discharging periods for dynamic network environments may help to achieve good energy management.

PROBLEM STATEMENT

The IoT environment relies heavily on WSNs to facilitate information exchange and seamless interaction among multiple devices. WSNs face numerous challenges that hinder their efficient operation, primarily related to energy consumption, network reliability, and QoS. Existing routing methods often struggle to address these complex issues, leading to reduced network lifespan and diminished efficiency. For IoT applications to perform optimally, QoS and network reliability are crucial, as they require consistent data transmission and low latency. Therefore, in IoT-enabled WSNs, there is an urgent need for an improved routing method that can ensure QoS, enhance system stability, and dynamically optimize energy usage. This study aims to tackle these challenges by developing a novel routing method that integrates QFO with Neuro-Fuzzy clustering. This comprehensive approach is designed to extend the lifespan and improve the efficiency of IoTenabled WSNs, addressing the critical needs for better path selection, QoS assurance, and energy optimization.

VII. MOTIVATION

Several major challenges hinder the effective implementation of WSNs in IoT environments particularly in terms of energy consumption, network reliability, and QoS. The dynamic and heterogeneous nature of IoT settings requires resilient and adaptable routing systems to ensure reliable and efficient data transmission. Traditional routing strategies often struggle to balance the conflicting demands of energy efficiency, reliability, and QoS, highlighting the need for novel approaches that can continuously adapt to changing network conditions and optimize resource utilization. Proposed solution lies in the combination of advanced techniques such as QFO and Neuro-Fuzzy Clustering. It can automatically group sensor nodes into energy-efficient clusters, while QFO optimizes routing paths by considering various factors such as trust metrics, QoS, and energy consumption. The goal of this study is to develop an energy-

aware, optimized routing method that leverages these cutting-edge techniques to enhance the lifespan and efficiency of IoT-enabled WSNs.

RESEARCH GAP

An energy-efficient clustered method is necessary from the standpoint of power-aware techniques, minimizing intercluster traffic in the entire network, and extending the lifespan of WSN. To improve safety, more attention must be paid to cloud computing and WSN integration for information aggregating and encrypted communication with the implementation of detection and prevention algorithms. The literature study makes clear that a variety of study efforts have been completed in the fields of safe transmission of data, energy-aware clustering remedies, and identifying attacks in sensor networks that are wireless. Numerous studies remain unanswered, particularly regarding the topics of group development, cluster head choosing, obtaining the best possible path, and identification of attacks and forecasting using bioinspired methods and deep learning-based security breach detection mechanisms to improve WSN efficiency.

VIII. LITERATURE REVIEW

Amir Masoud Rahmani et al.[1] The Internet of Things (IoT) plays a crucial role across diverse sectors such as industrial, educational, and healthcare. Ensuring stable and efficient network performance is essential for these applications, making optimal routing a critical factor. Proper clustering of network nodes is pivotal, as it enhances network efficiency and prolongs its lifetime by reducing energy consumption. This study proposes a novel routing approach for IoT networks based on Wireless Sensor Networks (WSN), called GWFCCV (Gray Wolf and Fuzzy Clustering and using Critic and Fuzzy Vikor approaches). Our method employs a combination of Gray Wolf Optimizer (GWO) and Fuzzy C-Means (FCM) for clustering, alongside multi-criteria decision-making techniques to rank and select nodes for efficient routing. Simulation results demonstrate that GWFCCV significantly improves key network parameters, including energy consumption, throughput, and network lifetime, outperforming existing approaches such as EACMRP-MS, FEEC-IIR, and FRLDG. For example, it can increase the lifetime of the network by 5.43 %, 8.3 % and 23.26 %, respectively.

Ahmed M. Khedr et al.[2] With the increasing complexity of dynamic and heterogeneous IoT-driven Wireless Sensor Networks (WSNs), context-aware routing has emerged as a promising approach to optimize network performance. These protocols improve Quality of Service (QoS), increase network lifespan, and improve energy efficiency by utilizing contextual data. However, they remain underexplored compared to traditional routing schemes. This survey presents the first comprehensive review in this area, addressing key research gaps by examining their evolution, methodologies, and performance over the past two decades. A novel classification framework is introduced, categorizing the protocols based on operational context and network characteristics, providing a structured view of their design.

Seyed Salar Sefati et al.[3] The Mobile Internet of Things (MIoT) represents a significant evolution of traditional IoT by enabling seamless connectivity for mobile devices and sensors in dynamic environments. Given the resource constraints and mobility challenges in MIoT networks, developing adaptive and energy-efficient routing strategies is important. This paper

proposes a novel routing protocol that integrates Grey Wolf Optimization (GWO) and Recurrent Neural Networks (RNNs) to enhance energy efficiency, reliability, and responsiveness in MIoT systems. The protocol features dynamic clustering, predictive traffic load balancing, and multi-objective optimization for Cluster Head (CH) selection, where RNNs forecast traffic trends and GWO optimizes routing paths.

A. Babu Karuppiah et al.[4] Wireless Sensor Networks (WSNs) are crucial in mission-driven domains such as environmental monitoring, industrial control, and military surveillance. However, their open communication medium, constrained resources, and unattended deployment make them prone to routing-layer attacks. Existing security frameworks mostly rely on reactive intrusion detection systems or conventional deep learning models, which incur high computational overhead and fail to adapt effectively under dynamic network conditions. To overcome these limitations, this study proposes a Neuro-Inspired Deep Learning Framework based on Spiking Neural Networks (SNNs) for autonomous intrusion prevention and energy-aware routing. The proposed model leverages latency-based spike encoding of key behavioral metrics (e.g., residual energy, latency, routing frequency, and packet delivery ratio) and utilizes a Leaky Integrate-and-Fire neuron architecture for proactive vulnerability prediction.

V. Nivedita et al.[5] Wireless Sensor Networks (WSN) and Mobile Ad Hoc Networks (MANET) are pivotal technologies widely used across various applications. However, the rise in wired and wireless technologies has also increased the frequency of attacks, compromising security, increasing packet loss, and reducing routing efficiency. Detecting denial-of-service (DoS) attacks remains a critical challenge, with issues in accuracy, scalability, and handling diverse attack methods. Existing methodologies face numerous challenges concerning the performance constraints of the detection system, the scalability and stability of the system, and the capacity to utilize extensive data effectively. To address these challenges, this research work proposes a cluster-based routing protocol integrated with a Stacked Convolutional Sequential Autoregressive Encoding Network (SCSAEN). The approach begins with density-based Adaptive Soft clustering (DAS) to maintain cluster stability during node mobility.

A. Chandra et al.[6] Mobile ad hoc wireless networks (MANETs) are decentralized, lacking fixed infrastructure, which enables dynamic and flexible communication between mobile nodes. However, these networks face challenges such as limited energy resources, frequent topology changes, and performance degradation caused by node misbehavior. Existing protocols like AODV have significant limitations, including a lack of energy awareness, an inability to detect malicious behavior, and the absence of secure transmission mechanisms. These weaknesses lead to rapid energy depletion and increased vulnerability to attacks. To address these issues, this paper proposes a novel energy-aware unobservable routing protocol.

Poornima M.R. et al.[7] The Internet of Things (IoT) is a paradigm in which real-world things are connected to the Internet for efficient processing, control, and communication without the need for human interaction. Due to the growing number of heterogeneous physical objects such as sensors, RFID, and other devices that are used in several IoT applications,

including health care, transportation, smart cities, industries, and other applications generate a large amount of data. To process this data over the network, energy-aware routing has become a critical issue because objects are equipped with energy-constrained batteries, which have a significant impact on the network's performance, quality, and lifetime.

Jay Kumar Jain et al.[8] Wireless communication is pivotal in the modern era, enabling seamless connectivity across diverse applications. However, the increasing complexity and sophistication of cyber threats pose significant challenges to the security of wireless communication systems. This paper proposes an innovative approach to enhance wireless communication security through integrating artificial intelligence (AI) techniques. First, we construct the network using the Horizontal Partitioning Sierpinski Triangle to reduce the network's high traffic and perform the authentication process. After successful authentication, we perform the clustering process and Game Theory-Driven Clustering (GT-DC) allows nodes to strategically optimize energy utilization while forming clusters as rational entities in a cooperative game.

Tayyab Khan et al.[9] Trust-based secure routing schemes are more effective than cryptographic routing protocols to convey energy-efficient data in WSNs since cryptographic protocols require high computation, more convergence time as well as storage space. The paper presents a well-organized trust estimation-based routing scheme (ETERS) that consists multi-trust (communication trust, energy trust, data trust) approach to alleviate several internal attacks like badmouthing, Sybil, selective forwarding, on–off, black hole, and gray-hole attacks for clustered WSN. The proposed multi-trust approach is used to analyze the credibility of sensitive monitored data.

Dr M. Anugraha et al.[10] A Mobile Ad-Hoc Network (MANET) represents a set of wireless networks that create the network without requiring centralized control. Moreover, the MANET serves as an effectual communication network but is impacted by security issues. MANET intrusion detection constantly monitors network traffic for potential intrusions. Still, it requires network nodes for analyzing, and processing the data, which leads to the highest processing charge. For solving such difficulties, the EIK Herd Anaconda Optimization (EHAO)-based routing, and EHAO-trained Deep Kronecker Network (EHAO-DKN) for intrusion detection is devised in this paper. The MANET simulation is the prime step for attaining the routing. The proposed EHGAO with the fitness factors are considered in the routing.

IX. CONCLUSION

This review paper presented a comprehensive study of the Fuzzy-ACO hybrid routing framework for enhancing the resilience and performance of AODV routing in IoT-enabled Wireless Sensor Networks (WSNs). The integration of Fuzzy Logic and Ant Colony Optimization (ACO) was found to significantly improve routing efficiency by intelligently selecting optimal paths under dynamic network conditions and link interference scenarios. The hybrid approach enhances packet delivery ratio, network stability, energy efficiency, and overall Quality of Service (QoS) while reducing packet loss, delay, and routing overhead. Furthermore, the review highlighted that combining intelligent decision-making with bio-inspired optimization provides a reliable solution for handling congestion, interference, and

node mobility in IoT-based WSN environments. The study concludes that the Fuzzy-ACO hybrid framework offers a promising and adaptive routing strategy for future resilient and energy-aware IoT communication systems.

REFERENCE

1. Rahmani, A. M., Haider, A., Ali, S., Mohammadi, M., Mehranzadeh, A., Khoshvaght, P., & Hosseinzadeh, M. (2025). A routing approach based on combination of gray wolf clustering and fuzzy clustering and using multi-criteria decision making approaches for WSN-IoT. Computers and Electrical Engineering, 122, 109946.
2. Khedr, A. M., Alfawaz, O., PV, P. R., & Osamy, W. (2025). Advancing IoT-driven WSNs with context-aware routing: A comprehensive review. Computer Science Review, 58, 100803.
3. Sefati, S. S., Maiduc, S. O., Arasteh, B., Larkotey, W. O., Bouyer, A., & Khan, W. U. (2025). Optimizing energy-efficient routing in Mobile internet of things (MIoT) networks using Grey wolf optimization and recurrent neural networks. Ad Hoc Networks, 104047.
4. Karuppiah, A. B., Nanjappan, V., RajaRaja, R., & Priyan, S. V. (2025). Neuro inspired deep learning based secure and energy efficient routing with autonomous intrusion prevention in wireless sensor networks. Engineering Applications of Artificial Intelligence, 162, 112783.
5. Nivedita, V., Shieh, C. S., & Horng, M. F. (2025). An integrated trust-based secure routing with intrusion detection for mobile Ad Hoc network using adaptive snow geese optimization algorithm. Ain Shams Engineering Journal, 16(7), 103385.
6. Chandra, A., & Chakravarthy, A. S. N. (2025). EAURP: An Energy-Efficient and Trust-Aware Unobservable Routing Protocol for Secure Mobile Ad Hoc Networks. Sustainable Computing: Informatics and Systems, 101285.
7. Poornima, M. R., Vimala, H. S., & Shreyas, J. (2023). Holistic survey on energy aware routing techniques for IoT applications. Journal of Network and Computer Applications, 213, 103584.
8. Jain, J. K., & Chauhan, D. (2025). Optimized secure and energy-efficient approach for IoT-enabled wireless sensor networks. Pervasive and Mobile Computing, 110, 102049.
9. Khan, T., Singh, K., Hasan, M. H., Ahmad, K., Reddy, G. T., Mohan, S., & Ahmadian, A. (2021). ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. Future Generation Computer Systems, 125, 921-943.
10. Anugraha, M., Ebenezer, S. S., & Maheswari, S. (2025). Hybrid Elk Herd Green Anaconda-Based Multipath Routing and Deep Learning-Based Intrusion Detection In MANET. Pervasive and Mobile Computing, 102079.
11. Mishra, R. (2024). Raspberry Pi Performance analysis across its Operating System in LED Control Operation. International Journal of Advanced Research and Multidisciplinary Trends (IJARMT), 1(2), 01-11.
12. Mishra, R. (2025). IOT and DSP (combination of hardcore Virtex-5 FPGA and soft core DSP processor) OFDM System PAPR Reduction Using Artificial Intelligence Algorithm. International Journal of Advanced Research and Multidisciplinary Trends (IJARMT), 2(1), 135-149.
13. Mishra, R., & Sharma, A. (2026). Enhanced Trajectory Tracking of a 6-DOF Robotic Manipulator Using GA–PID and ANN–PID Controllers. International Journal of Research & Technology, 14(2), 53-70.