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 of Secure Routing Optimization in IoT-Based WSN Using Particle Swarm Optimization

Harsh Nagar, Professor Amit Thakur
School Of Engineering and Technology, Vikram University, Ujjain University in Ujjain, Madhya Pradesh

ABSTRACT
The IoT can be defined as a system of various types of computing and digital devices, machines, objects, animals, and humans that are connected through networks to send data without the need for direct person-to person or computer-to-person interfaces. Every component in this structure is given a unique identity. While under the domain of IoT, WSN serves as a wireless sensor network that does not have an established infrastructure but consists of many wireless sensors for surveillance over systems, the environment, and the physical world. Because of its versatile usage like surveillance and environmental monitoring, Wireless Sensor Networks (WSNs) are vital in many applications. The performance of these networks is largely dependent on how sensor nodes are distributed across the area to provide good coverage and connectivity. In this paper, we propose a new method for node placement optimization in WSNs, which tries to solve the problem of coverage holes at the stage of initial deployment. Particle Swarm Optimization (PSO) are implemented using MATLAB to deal with the problem's complex and non-linear nature. These algorithms help find optimal node positions, thus improving coverage while ensuring no coverage gaps occur. A way to achieve this is through iterations, which involve fitness evaluation, selection of promising solutions, and genetic operators like crossover and mutation or position updates for PSO to investigate and improve the final solution. this demonstrate the usefulness of those methods, displaying major increases in coverage and the removal of all gaps that could appear in the initial deployment. This research contributes to the field of wireless sensor network optimization, specifically addressing coverage issues using GA and PSO algorithms.
Keywords: IoT; WSN; Genetic Algorithms; Particle Swarm Optimization; MATLAB

I. INTRODUCTION

In nature, many creatures—such as fishes, birds, and bees—have group behaviors. The abilities of individual members in a group are limited, but the whole group has a strong vitality. The strong vitality is not only a simple superposition of individual abilities but also an adjustment of individual behaviors through exchanging information, cooperating, and finally reflecting group intelligence.

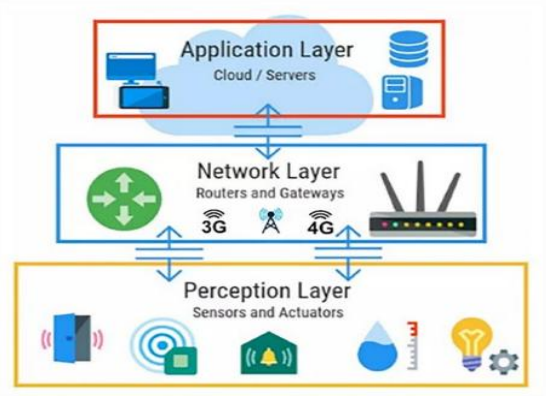
Swarm intelligence (SI) [1] algorithm is a simulation method to simulate biological group intelligence. The potential parallelism and distributed characteristics of SI algorithms enable the possibility of solving complex nonlinear problems with advanced capabilities in terms of self-adaptability, robustness, and search ability. Up to now, there are many SI-inspired optimization algorithms, such as classical particle swarm optimization (PSO) [2] and ant colony optimization (ACO) [3]. In recent years, there exist many improvements—such as

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

artificial bee colony (ABC) [4], bacterial foraging algorithm (BFO) [5], and butterfly optimization algorithm (BOA) [6]. SI algorithms search the optimized solution based on heuristic information. It can be applied to a wide variety of optimization problems (e.g., dynamic optimization problems, multi-objective optimization problems) and NP problems. With the ever-increasing development of IoT, SI exhibits great applicational prospect in IoT-related applications.

II. INTERNET OF THINGS

According to the text, Internet of Things (IoT) can be considered an important regional structure similar to normal systems where data can be transported and exchanged easily. Sometimes also called the "Internet of Everything," the IoT is a new paradigm in which information technologies like RFID, personal computers, the internet, embedded systems, communication technologies, and other devices are integrated to connect virtual and physical worlds [2], see Figure 1. What makes IoT so versatile is its readiness to adapt to almost every software part, hardware component, or sensor connected to its system. In the first place, the IoT plays a critical role in data and security management; it operates as an international channel linking people and things. Its usage is wide-ranging, starting from smart cities to quick medical support systems, smart buildings, and rapid transport response systems [3]. The possibility to eliminate multiple sensors by incorporating their functionalities into one simpler sensor exists within current IoT platforms [4]. This method requires an infrastructure-free wireless network called Wireless Sensor Network (WSN). WSN includes several wireless sensors that are placed strategically for tracking environmental, physical, and system variables [5]. The regional control and monitoring are achieved by sensor nodes possessing integrated CPUs, while these sensor nodes are associated with a central Base Station that acts as the WSN system's processing center. The base station links up to the Internet so that data can be shared [6]. In the realm of the IoT world, WSN applications are widespread and cover various sectors. Some of these areas involve security monitoring, surveillance, threat identification, military use cases, as well as environmental measurements which may include factors like air pressure, humidity, or temperature. WSNs provide significant value in different domains including patient monitoring in medicine, agriculture, and landslide detection. Nevertheless, adopting WSN comes with challenges such as limited power and energy resources; also security threats and QoS maintenance. These issues need to be addressed in order to fully exploit the potential of WSN within the larger context of IoT. [7], [8].



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: General IoT topology WSNs and the IoT have been explored extensively in the literature.

The research by S. W. Nourildean et al. evaluated the energy-efficient ZigBee WSNs, their routing topologies along with an investigation on applications and security issues of IoT-enabled WSNs [9]. On a separate note, V. Rishiwal et al. proposed a novel routing protocol and algorithm considering QoS factors to improve network performance within an IoT-based environment [1]. An important contribution to the field was made by T. Brito et al. when they proposed a novel encoding and decoding process to optimize communication in wireless sensor networks, which has been rarely addressed in the literature. Their approach was not merely theoretical; it was applied and validated in the practical context of a wildfire detection system [1].

III. PROBLEM DEFINITION

Utilizing clustering approaches has been demonstrated to be beneficial in developing sustainable routing solutions that take into account energy limits [16]. This technique classifies nodes into distinct groupings known as clusters. Appointed cluster heads (CHs) are in charge of managing clusters. These CHs collect participant data and transmit it to the sink [17, 18]. Clustering reduces the amount of transmission bandwidth used, promotes scalability, and resolves routing problems among sensors, as depicted in Fig. 1. Cluster heads (CHs) additionally filter and consolidate extraneous material from the gathered information, therefore decreasing the quantity of data packets transmitted to the central node. A network with n nodes that lacks clustering generates m packets per round, whereas a cluster-based network generates much fewer packets. More packets result in longer delays and higher energy consumption [2]. Network energy consumption also changes when the packet count being delivered to the sink rises since all nodes have the same destination [1]. The sink is unique in that it gathers all packets routed to it from the network, which reduces the longevity of the network. An energy-efficient routing protocol can balance traffic among nodes in the network [1]. This modification prevents potential failure by spreading out the data collection process equally among all nodes. This will increase the longevity of the network by reducing the burden on the central node, thus enhancing network connectivity and reliability [2].

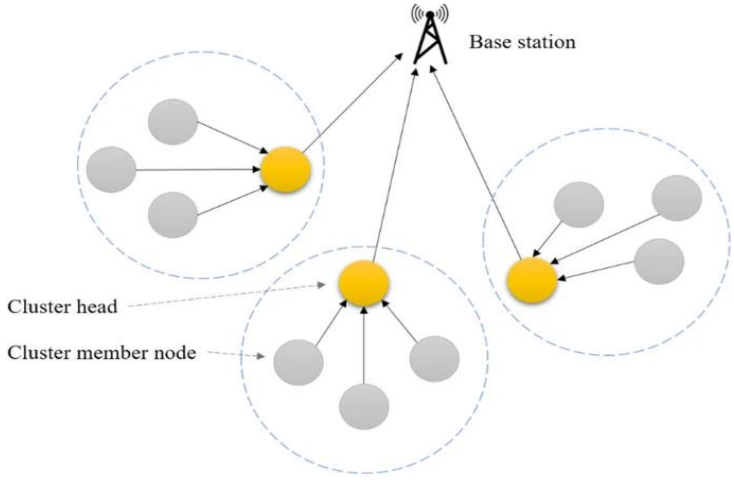


Fig.2.Clustering in a multi-hop WSN.

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

IOT ROUTING CHALLENGES

Routing in IoT networks encounters a number of distinct challenges due to the extensive size, diversity, limited resources, constantly changing topology, and varying demands of the applications. IoT networks may contain thousands of devices that need efficient communication. Conventional routing strategies cannot handle such vast networks because of their computational complexity and overhead [3]. Scalable routing algorithms are essential for managing the growing number of IoT devices and maintaining efficient data delivery. IoT devices possess diverse functionalities, employ multiple communication technologies, function within certain power constraints, and establish connections to networks through different methods. Routing algorithms must possess adaptability to effectively handle a variety of devices and make optimal routing decisions, considering the varied capabilities of devices and network conditions. Adaptive routing protocols, cross-layer optimization, and context-aware routing can be utilized to address the problem of heterogeneity effectively.

RESEARCH SIGNIFICANCE

Secure routing is a critical challenge in IoT-based Wireless Sensor Networks (WSNs) due to limited energy resources, dynamic network topology, and vulnerability to routing attacks. This research focuses on applying Particle Swarm Optimization (PSO) to enhance secure routing by optimally selecting energy-efficient and trustworthy paths for data transmission. By integrating security and optimization, the proposed approach aims to reduce energy consumption, improve network lifetime, and increase resistance against malicious nodes. The outcomes of this research contribute to reliable, scalable, and secure communication in IoT-enabled WSNs, which are essential for applications such as smart cities, healthcare monitoring, and industrial automation.

RESEARCH MOTIVATION

The rapid growth of IoT-based Wireless Sensor Networks has increased the demand for efficient and secure data communication. Traditional routing protocols in WSNs often fail to address security threats and energy constraints simultaneously, leading to reduced network lifetime and unreliable data delivery. Security attacks such as black hole, sinkhole, and selective forwarding further degrade network performance. These limitations motivate the use of intelligent optimization techniques like Particle Swarm Optimization (PSO) to design secure routing mechanisms. PSO offers fast convergence and adaptability, making it suitable for selecting optimal and secure routing paths in dynamic IoT-based WSN environments. This research is motivated by the need to develop a routing solution that balances security, energy efficiency, and network performance.

IV. LITERATURE REVIEW

Vidhya Sachithanandam et al.[1] Wireless Sensor Networks (WSNs) form the backbone of many key use cases, from environmental monitoring to healthcare to smart cities. But their use case is limited in terms of energy, latency, scalability, and security. To combat such problems, the paper suggests a new algorithm, the Energy-based Multi-Objective Donkey Smuggler Optimization Algorithm (EM-DSOA). This approach combines multi-aspect

optimization and a thin blockchain protocol, making it a one-stop shop to optimize WSN's efficiency, security, and stability. EM-DSOA as proposed optimizes energy utilization with dynamic clustering and adaptive routing with safe data transfer via blockchain integration. The approach is compared against current best practices like Multi Weight Chicken Swarm Based Genetic Algorithm (MWCSG) and Adaptive Hybrid Cuckoo Search and Grey Wolf Optimization (AHCS-GWO) by simulation examples of different network densities. The results are marked by significant improvement with energy efficiency of 99.13 %, packet loss reduction of 91 percent and throughput increase of 1000 %. The model likewise has very low end-to-end latency, which is perfect for real-time workloads. The study points out that EM-DSOA can be scalable and flexible, with a high performance across diverse and changing scenarios. With an eye towards energy efficiency, low latency and secure communications in the one, the proposed model takes WSN optimization to a new level of knowledge. This is a work that's not only up to the challenge of technology now but it also serves as a solid basis for future IoT and smart city deployments and will provide long-term, secure networks.

Oussama Senouci et al.[2] This paper addresses the challenge of energy-efficient and reliable data routing in Wireless Sensor Networks (WSNs) within Internet of Things (IoT) environments by optimizing the Expected Transmission Count (ETX) metric for efficient routing. Traditional ETX-based routing struggles with dynamic network conditions, leading to suboptimal path selection and increased energy consumption. To overcome these limitations, we propose a Machine Learning-Based ETX Optimization Approach, which dynamically adjusts ETX values based on real-time network conditions and historical transmission patterns. The approach employs a supervised learning model, specifically a CatBoost classifier, to predict the most energy-efficient and reliable routes. The model achieves a high classification accuracy of 98.9%, enabling precise differentiation between optimal and non-optimal links, thereby reducing retransmissions and balancing energy consumption across the network.

Ahmed Abdelaziz et al.[3] Determining the optimal configuration for wireless sensor networks (WSNs) can be challenging due to the multitude of possible setups. To address this issue, our team has developed the Parallel Particle Swarm Optimization-based Self-Organizing Network Clustering (PPSOPM) method. By taking into account variables like remaining node energy, predictable energy usage, proximity to the base station, and number of nearby nodes, PPSOPM dynamically enhances wireless sensor node clusters. Achieving a balance between these factors is crucial to effectively organize nodes into clusters and select a surrogate node as the cluster's head. In comparison to alternative methods, PPSOPM significantly improves network structure by 44.39 % and extends network lifespan. However, node density may impact network longevity by increasing the distance between nodes. Also, when the base station is far from the sensor area, creating additional clusters can help conserve energy. On average, PPSOPM requires 0.57 s to complete, with a standard deviation of 0.04.

Saugata Roy et al.[4] Due to autonomous flying ability and high manoeuvrability, unmanned aerial vehicle (UAV) assisted sensory data acquisition is becoming prevalent in outdoor IoT applications. However, UAV's limited onboard power source results in a restricted flight time, necessitating the use of a multi-UAV platform to ensure uninterrupted service in a large-scale

network. Nonetheless, very few studies have considered the use of multiple UAVs from distinct depots to improve network coverage with an optimal UAV swarm. This article investigates a multi-depot, energy-constrained vehicle routing problem (MDEVRP) where a fleet of UAVs is dispatched from different depots to collect sensory data from the ground nodes, provided that UAVs never run out of energy. Our objective is to discover an optimal set of UAVs with detailed hovering and travelling plans, which is an NP-hard problem. To solve such a computationally hard problem, we first leverage the variable dimensional particle swarm optimization (VD-PSO) algorithm that jointly optimizes the number of UAVs deployed, their depots, and association with the hovering locations. Then, minimal cost UAV trajectories are established, which preserves data freshness at the UAV depots. Simulation results manifest the dominance of the proposed scheme over the related state-of-the-art protocols.

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. The cluster head is selected using the Elk Herd Optimization (EHO) algorithm, which ensures resilience in dynamic MANET environments. The ASGO-TSPCPTrustNet algorithm performs in two ways: (i) Initially, the TrustSync Packet Control Protocol (TSPCP) computes the multi-attribute trust value to enhance network security; (ii) subsequently, the optimal route is determined utilizing the Adaptive Snow Geese Optimization Algorithm (ASGO). Additionally, SCSAEN-based intrusion detection is implemented to identify various attacks, including zero-day and DoS attacks.

Imtiaz Ahmad et al.[6] Numerous wireless networks have emerged that can be used for short communication ranges where the infrastructure-based networks may fail because of their installation and cost. One of them is a sensor network with embedded sensors working as the primary nodes, termed Wireless Sensor Networks (WSNs), in which numerous sensors are connected to at least one Base Station (BS). These sensors gather information from the environment and transmit it to a BS or gathering location. WSNs have several challenges, including throughput, energy usage, and network lifetime concerns. Different strategies have been applied to get over these restrictions. Clustering may, therefore, be thought of as the best way to solve such issues. Consequently, it is crucial to analyze effective Cluster Head (CH) selection to maximize efficiency throughput, extend the network lifetime, and minimize energy consumption.

Amruta Chandrakant Amune et al.[7] Security is the major issue that motivates multiple scholars to discover security solutions apart from the advantages of wireless sensor networks (WSN) such as strong compatibility, flexible communication and low cost. However, there exist a few challenges, such as the complexity of choosing the expected cluster, communication overhead, routing selection and the energy level that affects the entire communication. The ultimate aim of the research is to secure data communication in WSN using prairie indica optimization. Initially, the network simulator sets up clusters of sensor nodes. The simulator then selects the Cluster Head and optimizes routing using an advanced Prairie Indica Optimization algorithm to find the most efficient communication paths. Sensor nodes collect data, which is securely transmitted to the base station. By applying prairie indica optimization to WSNs, optimize key aspects of data communication, including secure routing and encryption, to protect sensitive information from potential threats.

Abdelali Hadir et al.[8] Sensor node localization is a critical issue in various Internet of Things (IoT) and Wireless Sensor Network (WSN) applications that require precise location data. Among the proposed solutions, the DV-Hop algorithm has been widely adopted to address this issue. However, achieving high localization accuracy remains a significant research challenge. This study introduces a novel approach to minimizing errors in estimating the average hop size using a new formula. Furthermore, the metaheuristic particle swarm optimization (PSO) is integrated into the DV-Hop method to refine the estimated locations of sensor nodes, enhancing localization accuracy. Extensive simulations demonstrate that the proposed technique outperforms several existing methods. The results indicate that the proposed approach significantly improves localization accuracy, with the ODV-HopPSO algorithm surpassing existing methods in terms of error reduction.

M.V. Srikanth et al.[9] Due to extremely unpredictable and diverse network traffic, the rapid expansion of IoT devices has increased security risks. Conventional IDS models frequently fall short of maintaining high accuracy when dealing with unbalanced datasets and changing attack types. In order to increase the effectiveness and precision of network intrusion detection, this research presents an intrusion detection system for IoT networks. The proposed system makes use of a hybrid whale optimization algorithm-particle swarm optimization (WOA-PSO) for feature selection and convolutional neural networks (CNN) for network traffic classification.

Kirandeep Kaur et al.[10] The Internet of Things (IoT) incorporates Wireless Sensor Networks (WSNs) to gather data in real time for a range of applications, including smart homes and healthcare. Energy efficiency is an essential concern considering sensor nodes have limited energy resources. Early node failures, network segmentation, and reduced quality of service (QoS) are driven by constant and uneven energy consumption among sensor nodes, particularly during data transmission and cluster head (CH) processes. For addressing this issue, the current study proposes a hybrid optimization approach for a clustering protocol that mitigates transmission latency and optimises energy efficiency by integrating bi-objective Tabu Search and Ant Colony Optimization (ACO). The primary goals include to extend the network lifetime via efficient data transmission and the most optimal possible cluster head (CH) selection.

V. CONCLUSION

This review paper presented a comprehensive analysis of secure routing optimization techniques in IoT-based Wireless Sensor Networks (WSNs) using Particle Swarm Optimization (PSO). The study highlighted that PSO-based routing approaches effectively improve network security, energy efficiency, routing stability, and data transmission reliability in dynamic IoT environments. By optimizing route selection and detecting malicious or unreliable nodes, PSO enhances packet delivery ratio, reduces delay, minimizes energy consumption, and prolongs network lifetime. The review also emphasized that integrating intelligent optimization techniques with secure routing mechanisms provides a robust solution against routing challenges and security threats in IoT-enabled WSNs. Overall, PSO-based secure routing is identified as a promising approach for developing reliable, scalable, and energy-aware next-generation IoT communication systems.

FUTURE SCOPE

Furthermore, the framework can enhance its autonomy and decision-making capabilities by incorporating machine learning methods like reinforcement learning. This enhancement would result in more efficient resource allocation and routing choices. Also, expanding the evaluation methodology to encompass real-life applications and other IoT situations would provide significant perspectives on the feasibility of the suggested strategy in different fields. By considering these possible future directions, progress in energy-efficient and scalable routing for IoT networks may be driven, ultimately enhancing the sustainability and longevity of IoT infrastructures.

REFERENCE

1. Sachithanandam, V., Jessintha, D., Subramani, H., & Saipriya, V. (2025). Blockchain integrated multi-objective optimization for energy efficient and secure routing in dynamic wireless sensor networks. Sustainable Computing: Informatics and Systems, 46, 101101.
2. Senouci, O., & Benaouda, N. (2025). Supervised machine learning-based ETX optimization for energy-efficient routing in IoT-enabled WSNs. Ad Hoc Networks, 103972.
3. Abdelaziz, A., Mahmoud, A. N., & Santos, V. (2025). A Parallel Particle Swarm Optimization for Improving Wireless Sensor Networks Longevity-Based Dynamic Clustering Method. Array, 100633.
4. Roy, S., Mazumdar, N., & Pamula, R. (2025). A multi-depot provisioned UAV swarm trajectory optimization scheme for collaborative data acquisition in a large-scale IoT environment. Ad Hoc Networks, 103974.
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. Ahmad, I., Hussain, T., Shah, B., Hussain, A., Ali, I., & Ali, F. (2024). Accelerated particle swarm optimization algorithm for efficient cluster head selection in WSN. Computers, Materials and Continua, 79(3), 3585.

7. Amune, A. C., & Pande, H. (2024). Secure data communication in WSN using Prairie Indica optimization. International Journal of Intelligent Unmanned Systems, 12(4), 377-398.
8. Hadir, A., Kaabouch, N., El Jamiy, F., & El Houssain, M. A. (2025). Optimized DV-Hop Localization Algorithm Using PSO for IoT and WSNs. Procedia Computer Science, 257, 690-697.
9. Srikanth, M. V., Sunitha, P., Kumar, A. S., & Akshaykranth, A. (2025). A Novel Framework for Intrusion Detection in IOT Networks using Hybrid Optimization Algorithm and Convolutional Neural Networks. Franklin Open, 100461.
10. Kaur, K., & Kaur, S. (2025). Hybrid Bio Inspired Optimization Based Routing Protocol For Enhancing Data Transmission In Clustered Network. Array, 100481.
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.