IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, May 2026
Impact Factor: 8.2

Energy Aware Clustering Routing Protocol for WSN Using Grey Wolf Optimization Algorithm: A Review

Himanshu Yadav and Sandeep Kumar
M.Tech Scholar, Department of CSE
Assistant Professor, Department of CSE
CBS group of Institutions, Village Fatehpuri, Jhajjar
himanshuyadav1600@gmail.com

Abstract: *Wireless Sensor Networks (WSNs) have become an essential technology in modern communication systems due to their applications in military surveillance, healthcare monitoring, environmental observation, industrial automation, and smart transportation systems. Despite their advantages, WSNs are highly vulnerable to security threats such as black hole attacks, packet dropping, intrusions, malicious node activities, and routing attacks because of their distributed architecture and limited resources. Ensuring secure and reliable communication in WSNs has therefore become a major research challenge.This review paper presents a detailed analysis of various intrusion detection systems (IDS), routing protocols, optimization techniques, and intelligent security mechanisms proposed for enhancing WSN security and performance. Different approaches including Direct Linear Genetic Programming (LGP), Multi Expression Programming (MEP), Gene Expression Programming (GEP), Extended Kalman Filter (EKF), Particle Swarm Optimization (PSO), Genetic Algorithms (GA), Fuzzy Logic Systems (FIS), stochastic Petri nets, Complex Event Processing (CEP), and AODV routing protocols have been studied and compared. The review also examines cross-layer detection systems, anomaly detection mechanisms, and black hole attack prevention methods used in WSN environments*

Keywords: WSN, IDS , PSO, GA, Fuzzy Logic System

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as one of the most important technologies in modern communication and monitoring systems due to their wide range of applications in military surveillance, healthcare monitoring, environmental sensing, industrial automation, smart agriculture, and intelligent transportation systems. A WSN consists of a large number of small sensor nodes that are deployed in a sensing environment to collect and transmit data to a base station. These sensor nodes are generally battery-powered and have limited energy, processing capability, memory, and communication range. Therefore, energy efficiency becomes one of the most critical challenges in the design and operation of WSNs.

Routing protocols play a significant role in improving network performance and extending the lifetime of sensor networks. Among various routing techniques, clustering-based routing protocols are widely preferred because they reduce communication overhead, improve scalability, and conserve energy. In clustering approaches, sensor nodes are grouped into clusters, and a cluster head is selected to collect and forward data from member nodes to the base station. Efficient cluster head selection is essential for minimizing energy consumption and balancing network load.

Recently, optimization algorithms inspired by nature have gained significant attention for solving complex routing and clustering problems in WSNs. One such intelligent optimization technique is Grey Wolf Optimization (GWO), which is based on the leadership hierarchy and hunting behavior of grey wolves in nature. The GWO algorithm provides

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, May 2026 Impact Factor: 8.2

efficient exploration and exploitation capabilities, making it highly suitable for cluster head selection and routing optimization in wireless sensor networks.

This review paper focuses on energy-aware clustering routing protocols for WSNs using the Grey Wolf Optimization algorithm. The study examines different clustering and routing approaches proposed by researchers to improve network lifetime, reduce energy consumption, enhance packet delivery ratio, and increase throughput. The review also analyzes the advantages, limitations, and performance of GWO-based routing protocols in comparison with traditional routing methods. Although GWO-based protocols show promising results in enhancing energy efficiency and network stability, several challenges still exist, including scalability issues, computational complexity, node mobility, and security vulnerabilities. Therefore, further research is required to develop adaptive, secure, and lightweight energy-aware routing mechanisms for next-generation wireless sensor networks.

II. LITERATURE REVIEW

M. Kocakulak and I. Butun (2017) presented an overview of Wireless Sensor Networks toward IoT applications. The study discussed WSN architecture, communication challenges, energy constraints, and future research directions for IoT-based sensor networks.

Muhammad Saqib et al. (2019) proposed security approaches for Software-Defined Wireless Sensor Networks (SDWSN). Their study focused on intrusion detection systems, security threats, and network protection mechanisms for resource-constrained WSNs.

E. Baraneetharan (2020) reviewed machine learning-based intrusion detection techniques for WSNs. The research highlighted the importance of intelligent IDS systems for detecting attacks and improving network security in wireless sensor environments.

Zainab Alansari et al. (2022) conducted a systematic review of routing attack detection methods in WSNs. The study analyzed routing attacks, malicious node behavior, and security solutions for enhancing secure communication in sensor networks.

Anita and Amita Asthana (2023) reviewed various routing protocols in WSNs and identified open research challenges. Their work focused on dynamic routing, energy-efficient communication, LEACH, TEEN, and APTEEN routing mechanisms.

Mohammed Faris et al. (2023) presented a recent review on WSN security based on state-of-the-art techniques. The study discussed different types of attacks, security challenges, and defense mechanisms in wireless sensor networks.

Dukka Karun Kumar Reddy et al. (2024) carried out a systematic literature review on swarm intelligence-based intrusion detection systems. Their research emphasized the effectiveness of swarm intelligence algorithms in improving IDS performance and network security in WSNs.

Ahmed A. Al-Healy and Qutaiba I. Ali (2024) reviewed WSN routing protocols focusing on energy efficiency, scalability, and reliable data transmission. The study highlighted the importance of efficient routing for extending network lifetime.

Doaa A. Hamdi et al. (2026) conducted a systematic review on deep learning-driven intrusion detection systems for software-defined WSNs. The study explored AI-based IDS models, deep learning techniques, and intelligent security frameworks for improving attack detection accuracy and network reliability.

Wireless Sensor Networks research from 2017–2026 shows significant progress in routing protocols, intrusion detection systems, swarm intelligence, fuzzy logic, machine learning, and deep learning techniques. Current research trends focus on energy-efficient clustering, intelligent optimization algorithms, secure communication, and AI-driven adaptive routing mechanisms for next-generation WSN applications.

WSN Protocols

Wireless Sensor Networks (WSNs) use different communication and routing protocols to ensure efficient data transmission, energy conservation, scalability, reliability, and network security. Since sensor nodes have limited battery

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, May 2026 Impact Factor: 8.2

power, memory, and processing capability, WSN protocols are specially designed to optimize energy consumption and improve network lifetime. These protocols are generally classified into routing protocols, MAC protocols, transport protocols, and security protocols.

1. Routing Protocols in WSN

Routing protocols are responsible for selecting efficient paths for transmitting sensed data from sensor nodes to the base station.

a) LEACH (Low Energy Adaptive Clustering Hierarchy)

LEACH (Low Energy Adaptive Clustering Hierarchy) is one of the most widely used hierarchical routing protocols in Wireless Sensor Networks. The protocol is designed to improve energy efficiency and extend the lifetime of wireless sensor networks by using a clustering mechanism. In LEACH, sensor nodes are grouped into clusters, and a cluster head is selected periodically among the nodes. The cluster head is responsible for collecting data from member nodes, aggregating the information, and transmitting it to the base station. The periodic and randomized selection of cluster heads helps distribute energy consumption evenly among sensor nodes, thereby reducing the chances of early node failure. LEACH significantly reduces communication overhead and minimizes direct transmission between individual sensor nodes and the base station. As a result, it improves network lifetime and conserves energy effectively. However, LEACH also has certain limitations. The protocol is not suitable for large-scale wireless sensor networks because of scalability issues, and the random cluster head selection process may lead to uneven cluster distribution, which can affect overall network performance and energy balance.

b) PEGASIS (Power-Efficient Gathering in Sensor Information Systems)

PEGASIS (Power-Efficient Gathering in Sensor Information Systems) is an improved routing protocol developed to overcome some of the limitations of the LEACH protocol in Wireless Sensor Networks. Instead of forming clusters, PEGASIS organizes sensor nodes into a communication chain where each node communicates only with its nearest neighboring node. In this protocol, data is passed sequentially from one node to another along the chain, and finally, only one selected node transmits the aggregated data to the base station. This chain-based communication mechanism significantly reduces the number of long-distance transmissions, resulting in lower energy consumption and improved network lifetime. PEGASIS effectively balances energy usage among sensor nodes and enhances overall network efficiency. However, the protocol also has certain drawbacks. Since data must travel through multiple nodes in the chain before reaching the base station, transmission delay increases, especially in large networks. Additionally, the process of forming and maintaining the communication chain becomes complex when the network size increases or node mobility occurs.

c) TEEN (Threshold Sensitive Energy Efficient Sensor Network)

TEEN (Threshold Sensitive Energy Efficient Sensor Network) is a hierarchical routing protocol designed specifically for time-critical applications in Wireless Sensor Networks. The protocol uses a reactive routing approach in which sensor nodes transmit data only when certain predefined threshold values are reached. TEEN introduces two types of thresholds, namely hard threshold and soft threshold, to control data transmission efficiently. This threshold-based communication mechanism helps reduce unnecessary transmissions and conserve the energy of sensor nodes. TEEN is highly suitable for applications that require immediate response to sudden changes or critical events, such as environmental monitoring, military surveillance, and disaster detection systems. Due to its event-driven communication process, the protocol significantly improves energy efficiency and extends network lifetime. However, TEEN also has certain limitations. Since data is transmitted only when threshold conditions are met, the protocol is not appropriate for continuous monitoring applications where regular data reporting is necessary.

d) APTEEN (Adaptive Periodic TEEN)

APTEEN (Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network) is an advanced routing protocol developed for Wireless Sensor Networks that combines both proactive and reactive routing mechanisms. The protocol is designed to provide periodic as well as event-driven data reporting, making it more flexible and efficient than TEEN. In APTEEN, sensor nodes transmit data periodically while also responding immediately when critical threshold

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, May 2026 Impact Factor: 8.2

conditions occur. This hybrid communication approach allows the protocol to support real-time applications and continuous monitoring simultaneously. APTEEN improves energy efficiency by reducing unnecessary data transmissions and optimizing communication among sensor nodes. It is highly suitable for applications requiring both regular monitoring and rapid event detection, such as environmental monitoring, healthcare systems, and industrial automation. However, the protocol also has certain limitations. Due to the integration of multiple communication mechanisms and threshold management processes, APTEEN becomes more complex in terms of implementation, routing management, and network maintenance compared to simpler routing protocols.

2. MAC Protocols in WSN

MAC (Medium Access Control) protocols control channel access and reduce collisions.

a) S-MAC (Sensor MAC)

S-MAC (Sensor Medium Access Control) is a MAC protocol designed for Wireless Sensor Networks to reduce idle listening and conserve the energy of sensor nodes. In wireless sensor networks, idle listening consumes a significant amount of battery power because sensor nodes continuously remain active while waiting for possible communication. S-MAC addresses this issue by introducing periodic sleep and wake-up schedules, allowing nodes to switch to sleep mode when communication is not required. This mechanism significantly reduces unnecessary energy consumption and minimizes packet collisions during data transmission. As a result, S-MAC improves energy conservation and extends the overall network lifetime. However, the protocol also has certain limitations. Since nodes remain in sleep mode for specific periods, data transmission may experience increased latency, especially in time-sensitive applications where immediate communication is necessary.

b) T-MAC (Timeout MAC)

T-MAC (Timeout Medium Access Control) is an improved version of the S-MAC protocol designed for Wireless Sensor Networks. The protocol enhances energy conservation by dynamically adjusting the active and sleep periods of sensor nodes according to network traffic conditions. Unlike S-MAC, where fixed sleep schedules are used, T-MAC allows nodes to enter sleep mode when no communication activity is detected for a certain timeout period. This adaptive communication mechanism helps reduce unnecessary energy consumption and improves overall network efficiency. T-MAC is highly effective in networks with variable traffic loads because it provides better energy efficiency and flexible communication management. However, the protocol also faces a limitation known as the “early sleeping problem,” where a sensor node may go into sleep mode too early before receiving important data from neighboring nodes, which can affect communication reliability and data transmission performance.

III. CONCLUSION

Wireless Sensor Networks play a vital role in modern monitoring and communication systems, but energy limitations and security challenges affect their performance. This study reviewed important routing and MAC protocols such as LEACH, PEGASIS, TEEN, APTEEN, S-MAC, and T-MAC used for improving energy efficiency and communication reliability in WSNs. The review highlighted that clustering, chain-based routing, and intelligent optimization techniques like Grey Wolf Optimization significantly enhance network lifetime and efficiency. However, issues such as scalability, delay, and security threats still exist, requiring future development of adaptive, secure, and energy-efficient routing protocols.

REFERENCES

[1]. Hafiza Syeda Zainab Kazmi, Nadeem Javaid “Congestion Control in Wireless Sensor Networks based on Support Vector Machine, Grey Wolf Optimization and Differential Evolution ”Wireless Days, WD, IFIP , pp 1-8 , 2025.

[2]. SatyasenPanda , Sweta Srivastava , Santosh Mohapatra “Performance analysis of wireless sensor networks using Artificial Bee Colony algorithm ” IEEE International Conference on Technologies for Smart-City Energy Security and Power (ICSESP-2018), pp 56-61March 28-30, 2024, Bhubaneswar, India.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, May 2026
Impact Factor: 8.2

[3]. Halil Yetgin ; Kent Tsz Kan Cheung ; Mohammed El-Hajjar ; Lajos Hanzo Hanzo "A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks" in IEEE Communications Surveys & Tutorials (Volume: 19 , Issue: 2 , Second quarter 2023

[4]. G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song and S. H. Ahmed, "Energy Efficient Direction-Based PDORP Routing Protocol for WSN," in IEEE Access, vol. 4, no. , pp. 3182-3194, 2022.

[5]. Q. Yu, Z. Luo and P. Min, "Intrusion detection in wireless sensor networks for destructive intruders," 2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Hong Kong, 2015, pp. 68-75.

[6]. S. Rani, J. Malhotra, and R. Talwar, ''Energy efficient chain based cooper-ative routing protocol for WSN,'' Appl. Soft Comput., vol. 35, pp. 386–397,Oct. 2020.

[7]. Jain and B. V. R. Reddy,P. R. Vamsi and K. Kant ''A novel method of modeling wireless sensor network using fuzzy graph and energy efficient fuzzy basedk-hop clustering algorithm,'' Wireless Pers. Commun., vol. 82, no. 1,pp. 157–181, 2020

[8]. C.V.Anchugam," Detection Approach for Black Hole Attack on AODV in MANETs using Fuzzy Logic System" International Journal of Advanced Information Science and Technology Vol.33, No.33, January 2019.

[9]. P. R. Vamsi and K. Kant, "Secure data aggregation and intrusion detection in wireless sensor networks," 2015 International Conference on Signal Processing and Communication (ICSC), Noida, 2015, pp. 127-131.

[10]. H. Yetgin, K. T. K. Cheung, M. El-Hajjar, L. Hanzo, "Network-lifetime maximization of wireless sensor networks", IEEE Access, vol. 3, pp. 2191-2226, Nov. 2015.

[11]. Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos, Felix C. Freiling and Tassos Dimitriou, "Cooperative Intrusion Detection in Wireless Sensor Networks." European Conference on Wireless Sensor Networks, pp 263-278, 2015.

[12]. Anbumozhi, K.Muneeswaran, Sivakasi, "Detection of Intruders in Wireless Sensor Networks Using Anomaly," International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.

[13]. Butun, S. D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 266-282, First Quarter 2014

[14]. Joseph Rish Simenthy CEng , AMIE, K. Vijayan, "Advanced Intrusion Detection System for Wireless," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, an ISO 3297: 2007 Certified Organization Vol. 3, Special Issue 3, April 2014.

[15]. Harmandeep Kaur, "A Novel Approach To Prevent Black Hole Attack In Wireless Sensor Network" International Journal For Advance Research In Engineering And Technology, Vol. 2, Issue VI, June 2014.