International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

Review and Optimization of Clustering and Routing Protocols in Wireless Sensor Networks

Jyoti
M Tech Student, CDLU, Sirsa
Jyotisrs92@gmail.com

Vikram Singh
Department of Computer Science and Engineering, Chaudhary Devi Lal University, India

Sikander
scientistsikander@gmail.com

Abstract: The past few years have witnessed increased interest in the potential use of wireless sensor networks (WSNs) in a wide range of applications and it has become a hot research area. Based on network structure, routing protocols in WSNs can be divided into two categories: flat routing and hierarchical or clustering routing. Owing to a variety of advantages, clustering is becoming an active branch of routing technology in WSNs. In this paper, we present a comprehensive and fine grained survey on clustering routing protocols proposed in the literature for WSNs. the advantages and objectives of clustering for WSNs, and develop a novel taxonomy of WSN clustering routing methods based on complete and detailed clustering attributes. In particular systematically analyze a few prominent WSN clustering routing protocols and compare these different approaches according to our taxonomy and several significant metrics. Finally, we summarize and conclude the paper with some future directions.

Keywords: wireless sensor networks; clustering routing; cluster construction; data transmission;

I INTRODUCTION

In the wake of the "sensor city" movement, wireless sensor networks (WSN) have found numerous applications in fields as diverse as urban planning, environmental monitoring, healthcare, agriculture, industry, and the military and national defense. They are also used in smart homes and other human-centric applications. A collection of sensor nodes dispersed at random makes up the WSN, making it an ad hoc network [1]. Nodes are able to gather, process, and transmit data because they perceive their surroundings. Unfortunately, WSN sensor nodes utilize limited energy (like batteries), and it might be challenging to provide power in certain complicated work conditions, which can result in the network's unreliability in terms of longevity and quality. Further, how to manage node energy consumption is much more important for situations with high real-time requirements [2]. These scenarios include disaster monitoring, military supervision,

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

medical inspection, and many more. So, WSN research focuses on finding a compromise between energy usage and network lifetime extension.

To ensure effective communication in WSN, routing methods must carefully pick cluster head (CH) nodes. Because of their superior energy usage, CH nodes are responsible for data gathering, data fusion, and data transmission within the cluster. All of the sensor nodes can make better use of the available power if a clustering protocol is well-designed. There are four steps to the clustering routing protocol: selecting a cluster head, forming clusters, merging data, and sending data. The whole network is partitioned into several clusters. For each cluster, choose one node to serve as the CH and the others as the CM. With the help of the CH node in each cluster, the CM nodes exchange data and communicate with it. As illustrated in Figure 1, the data is sent from the CH nodes to the sink node, which subsequently integrates it and sends it to the network for user-to-user communication management [3]. Moreover, routing clustering algorithms do not perform well in heterogeneous networks; hence research centered on these protocols is currently a hotspot for heterogeneous network research.

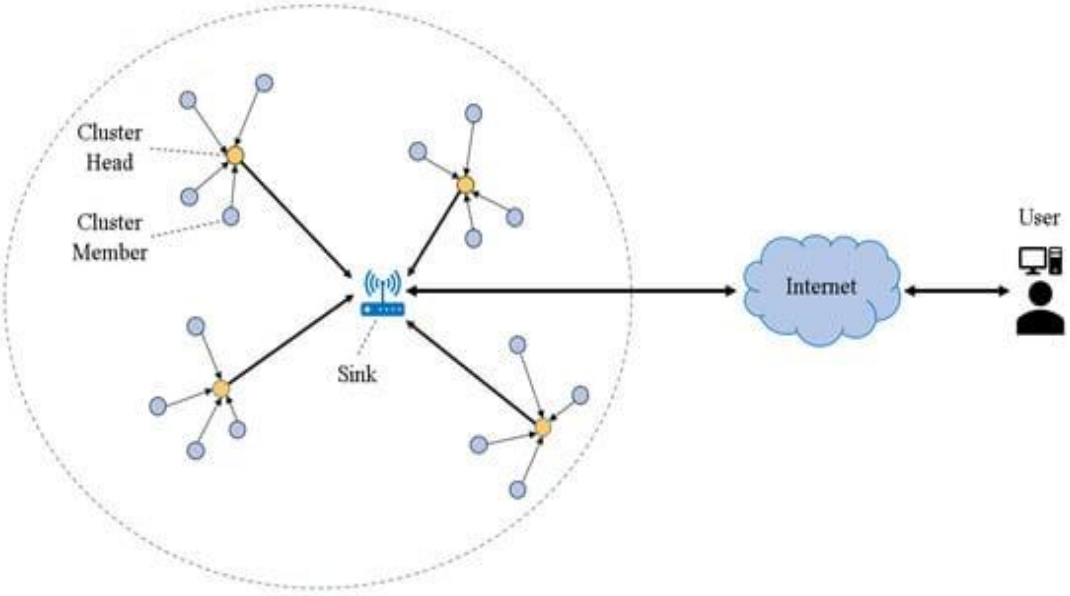

Figure 1. Clustered routing structure of WSN.

Research in the field has long focused on developing cluster routing protocols using the metaheuristic algorithm [4]. For difficult optimization tasks, the metaheuristic algorithm is an effective tool. More complicated NP-hard problems can have their best approximation solved in polynomial time using it [6]. Metaheuristic algorithms are being proposed in rapid succession as bionics research progresses; for instance, the grey wolf optimizer (GWO) [6], the seagull optimization algorithm (SOA), the bat algorithm (BA), the genetic algorithm (GA) and many

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

more. Mathematical processes like adding, subtracting, multiplying, and dividing constitute the basis of the formulas for the individual steps of numerous metaheuristic algorithms. Neither the mathematical model of the algorithm nor any particular scientific theory provides a strong connection to reality. They looked for formula derivation on the biological development principle of bamboo forests in order to develop a metaheuristic algorithm that is both highly effective and closely related to the mathematical model of reality. This study presents a novel metaheuristic optimization algorithm called the bamboo forest growth optimizer (BFGO). It is based on the differential model of bamboo growth and the Gaussian mixture models. The optimization ability of the algorithm is demonstrated on the CEC test sets and engineering optimization problems.

II ROUTING PROTOCOLS

Routing Protocols in Wireless Sensor Networks

The purpose of routing is to determine the best way to go from one node to another [7]. Because WSNs are fundamentally different from conventional networks, routing in them is extremely difficult. A number of critical aspects influence the design of WSN routing protocols. By addressing these characteristics, WSNs can achieve effective communication.

Classification of Routing Protocols in WSNs

In WSNs, the network layer is used to implement the routing of incoming data. In multi-hop networks, the source node cannot reach the sink directly. So, intermediate nodes have to relay their packets. The implementation of routing tables gives the solution. WSN routing protocols can be classified into five ways, according to the way of establishing the routing paths, according to the network structure, according to the protocol operation, according to the initiator of communications, and according to how a protocol selects a next hop on route of forwarded message. The taxonomy of routing protocols is shown in figure 2.

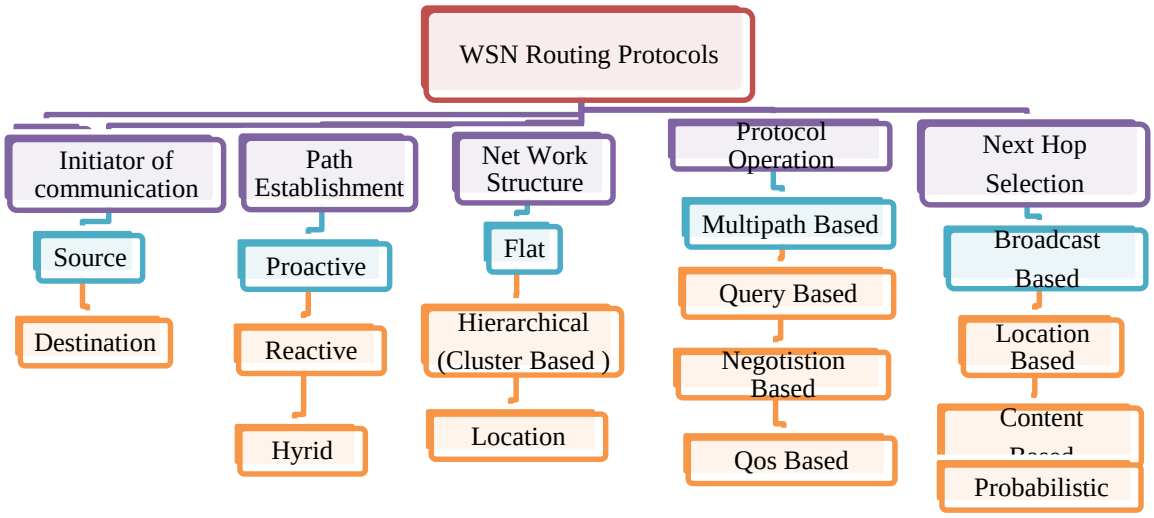

Figure.2. Taxonomy of routing protocols in WSNs

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

The network structure based routing protocols are categorized as: flat based, hierarchal based (cluster based), and location based routing protocols. In flat based routing, every sensor node plays same role. While, in hierarchal based routing, sensor nodes have different roles. So, when network scalability and efficient communication is needed, hierarchal or cluster based routing is the best choice.

Routing Protocols in Wireless Sensor Networks

Routing is a method to find out a path between the source node and the destination node [8]. Routing in WSN is really challenging due to the intrinsic characteristics that differentiate these networks from other networks. The design of routing protocols in WSNs is affected by several exigent factors. The efficient communication can be achieved in WSNs by overcoming these factors.

Here's a comprehensive table that includes various **Routing Protocols in Wireless Sensor Networks (WSNs),** including **Open Shortest Path First (OSPF)** and **Routing Information Protocol (RIP)**, along with additional routing protocols. The table highlights their characteristics across **Energy Efficiency, Delivery Delay, Cluster Stability, Scalability, Load Balancing,** and **Algorithm Complexity**.

Table 1 comparison different routing protocols

Routing Protocol	Energy Efficiency	Delivery Delay	Cluster Stability	Scalability	Load Balancing	Algorithm Complexity
LEACH	High	Moderate	Low	Moderate	Moderate	Low
PEGASIS	High	Low	Moderate	Moderate	High	Moderate
D2CRP	Moderate	Moderate	Moderate	Moderate	Moderate	Low
HEED	High	Low	Moderate	High	High	Moderate
UCR	Moderate	Moderate	High	Moderate	High	Moderate
MBC	Moderate	Moderate	Moderate	Good	Moderate	Moderate
FLOC	Moderate	Low	High	Moderate	High	Moderate
DBSCAN	Moderate	Moderate	High	Limited	Moderate	Moderate
GA-LEACH	High	Low	Moderate	Good	High	High
PSO-C	High	Low	High	Good	High	High
ACO-C	Moderate	Moderate	High	Moderate	High	Moderate
Fuzzy LEACH	High	Moderate	Moderate	Good	Good	Moderate
OSPF	Moderate	Low	High	High	Moderate	High

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

RIP	High	Moderate	High	Good	Good	Moderate
AODV	Moderate	Moderate	Moderate	Good	Moderate	Moderate

Design Challenges of Routing Protocols in WSNs

To provide dependable and efficient communication in WSNs, routing protocols [9] are tasked with finding and maintaining energy-efficient paths inside the networks. Because of the constraints of the network type, the primary goal of routing protocol design is to maximize the lifetime of the network by minimizing power consumption by the sensors. The network remains connected for an extended duration due to this issue. While developing routing protocols, it is vital to keep in mind a number of difficult aspects. Here they are:

Depending on the application, node deployment might have a significant impact on routing protocol performance. Two such approaches are manual and randomized [10]. Data is routed along predetermined paths in the first technique, which involves manually placing the nodes. Careful selection of node density ensures coverage of area during manual deployment. When nodes are expensive and their positions affect their operations, this is a reasonable solution; nonetheless, it is not suitable for hard settings [11]. In contrast, nodes are dispersed at random during random deployment. Having a random node deployment to produce effective results is efficient when the application is related to event detection [12].

Energy consumption: The primary objective of routing protocols is to efficiently transmit data between sensors and the sink. As it takes in data, processes it, sends it out, and receives it, every sensor node uses energy. The activity that uses the most energy is transmitting data Due to the finite energy resources of the sensor nodes, when some of them run out of juice, the entire network has to be restructured, new paths have to be discovered, and topology changes occur. Therefore, it is necessary to develop routing protocols that can balance the two competing goals of energy efficiency and precision.

Nature of node: Nodes in a WSN can be homogeneous or heterogeneous depending on the environment. In contrast to heterogeneous nodes, which have varying capacities, homogeneous nodes share characteristics like computing power, battery life, and transmission range. Most network designs work under the assumption that sensor nodes would remain in one place. But in a few of uses, both the base stations and the nodes need to be mobile.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

Coverage: In WSNs, every node has its own perspective on the surrounding world. The range and precision of every one sensor's view of its surroundings are finite. So, covering area is a crucial concern in design [14].

Scalability: There might be anywhere from a few hundred to thousands of nodes out in the field. It is necessary for the routing protocol to support a large number of nodes [15]. It becomes impractical for every node to have an exhaustive understanding of the network topology when the number of nodes is large.

Quality of service (QoS): The application's necessary level of quality of service should be met by the routing protocols. Broadband, delivery latency, throughput, jitter, and so on are all examples of quality of service metrics Applications that detect and track targets, for example, necessitate time-sensitive data with minimal transmission delays. Nevertheless, high throughput is necessary for multimedia networks.

Application: All applications have their own unique routing protocols. That is to say, various scenarios and network conditions call for distinct routing protocols. From the perspective of the application, there are a number of ways to gather data from the environment. These include time-driven, event-driven, and query-driven approaches. The sensor nodes in a time-driven system communicate with base stations or gateways at regular intervals. When an event happens, sensor nodes in an event-driven system report the data they've acquired. In query driven techniques, the BS eventually sends a query to the nodes in order to seek their data [17].

III CLUSTERING

There are a lot of sensors in a WSN, but the battery life is short. While it's true that WSN hubs can function in potentially dangerous environments, recharging or replacing the battery becomes impossible in such settings. Therefore, the network cannot function without energy saving. When constructing a routing protocol, energy consumption is typically the first factor to be considered. Routing methods can significantly impact energy utilization.

If the aim is for the system to last longer and use less power from your sensors, cluster-based routing methods are a good bet. In most cases, clusters of sensor hubs are avoided. This set makes use of both member hubs, referred to as ordinary nodes (ON), and an exceptional hub, the cluster head (CH). In addition to collecting data and transmitting it to the base station (BS), the CH can choose high energy With this protocol, sensor hubs can send detected data to the appropriate CH while reducing the number of messages passing through the system [18]. Based on the chosen WSN architecture, the BS can access data from any CH in the network through an intermediary CH.In order to eliminate redundant data and transmit just the most explicit information, the CH first accepts data from the cluster member and then performs sensors on that data. Since energy consumption is seen as a primary determinant in WSN selection, this transmission type is employed to conserve energy.In most cases, clustering methods greatly decrease radio

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

transmissions while simultaneously increasing scalability. Providing a solution that keeps sensor reliability throughout the system's activity is a clear objective of clustering.

Benefits of Clustering in WSN

Optimal management approaches can be implemented in the network using clustering. Clusters handle network topology and communication overhead at the sensor level due to hub associations with just CHs. Maintaining communication capacity and preventing exchange message redundancy are two benefits of clustering [18].

Cluster-Based Routing Protocol Classification—Overview

There are three distinct kinds of clustering :(1) parameter-based, (2) optimization-based, and (3) methodology-based. The first way to look at parameter-based clustering is as two main categories: clustering based on primary parameters and clustering based on secondary parameters. Second, there are two main schools of thought when it comes to optimization-based clustering: the classical school and the hybrid school. At last, as shown in Figure 3, methodology-based clustering is further classified into metaheuristic approaches and fuzzy-based methods. In Section 4, we go over each of these categories in detail.

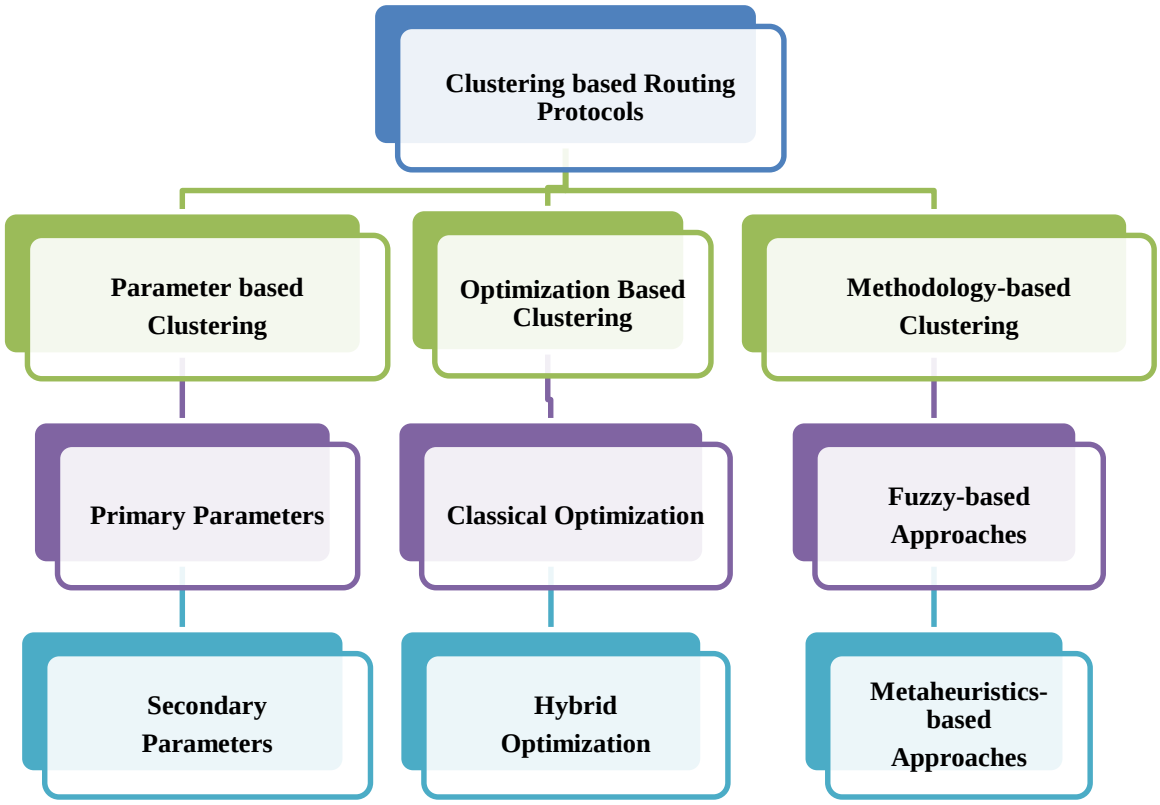

Figure 3. Classification of clustering-based routing protocols.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

Table 2 comparison Clustering Protocol with performance matrix

Clustering Protocol	Energy Efficiency	Delivery Delay	Cluster Stability	Scalability	Load Balancing	Algorithm Complexity
LEACH (Low-Energy Adaptive Clustering Hierarchy)	High	Moderate	Low	Moderate	Moderate	Low
PEGASIS (Power-Efficient GAthering in Sensor Information Systems)	High	Low	Moderate	Moderate	High	Moderate
D2CRP (Distributed 2-Hop Clustering Protocol)	High	Moderate	High	Good	Good	Moderate
HEED (Hybrid Energy-Efficient Distributed Clustering)	High	Low	Moderate	High	High	Moderate
UCR (Unequal Clustering Routing)	Moderate	Moderate	High	Moderate	High	Moderate
MBC (Mobility-Based Clustering)	Moderate	Moderate	Moderate	Good	Moderate	Moderate
FLOC (Fast Local Clustering)	Moderate	Low	High	Moderate	High	Moderate

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

DBSCAN (Density-Based Spatial Clustering)	Moderate	Moderate	High	Limited	Moderate	Moderate
GA-LEACH (Genetic Algorithm optimized LEACH)	High	Low	Moderate	Good	High	High
PSO-C (Particle Swarm Optimization Clustering)	High	Low	High	Good	High	High
ACO-C (Ant Colony Optimization Clustering)	Moderate	Moderate	High	Moderate	High	Moderate
Fuzzy LEACH	High	Moderate	Moderate	Good	Good	Moderate

Design Challenges of Routing Protocols in WSNs

To provide dependable and efficient communication in WSNs, routing protocols are tasked with finding and maintaining energy-efficient paths inside the networks. Because of the constraints of the network type, the primary goal of routing protocol design is to maximize the lifetime of the network by minimizing power consumption by the sensors. The network remains connected for an extended duration due to this issue. While developing routing protocols, it is vital to keep in mind a number of difficult aspects. Here they are:

Node deployment: The effectiveness of the routing protocols is impacted by deployment, which is highly application-specific. Randomization and manual processes are both possible [19]. The first approach involves physically placing the nodes and then routing data along predetermined pathways. With manual deployment, the coverage of a region is achieved by selecting the node density with care. This is a useful option when nodes are expensive and their location affects their operations, but it won't hold up well in extreme conditions.But in random deployment, the placement of the nodes is completely at random. An efficient use case for random node deployment to get effective results is in event detection applications.

Energy consumption: Transmitting data between sensors in an inefficient way is the primary goal of routing protocols. When sensing, processing, receiving, or transferring data, each sensor node uses energy. Out of all these tasks, transmitting data uses the most energy.Due to the finite energy

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

resources of the sensor nodes, drastic changes in the network's topology and connection, as well as the need to reorganize the network and discover new paths, are inevitable consequences of power outages. Since energy optimization and accuracy are two competing goals, routing techniques that strike a balance between the two are necessary.

Nature of node: Nodes in a WSN can be homogenous or heterogeneous depending on the environment. In contrast to heterogeneous nodes, which have varying capacities, homogeneous nodes share characteristics like computing power, battery life, and transmission range. Most network designs work under the assumption that sensor nodes would remain in one place. But in a few of uses, both the base stations and the nodes need to be mobile [14].

Coverage: Every node in a WSN has its own unique perspective on the world around it. There are range and accuracy limitations to what a particular sensor can see in its surroundings. Accordingly, the coverage area is a crucial concern in the design process [11].

Scalability: In the field, the number of nodes might range from a few hundred to several thousand. In order for the routing protocol to function, it must be capable of handling a large number of nodes. Every node needs to know the network topology on a global scale, however this becomes impractical when the number of nodes is large.

Quality of service (QoS): The application's necessary level of quality of service should be met by the routing protocols. Broadband, delivery latency, throughput, jitter, and so on are all examples of quality of service metrics. Applications that detect and track targets, for example, necessitate time-sensitive data with minimal transmission delays. Nevertheless, high throughput is necessary for multimedia networks.

Application: The routing protocols are highly context dependent. That is to say, various scenarios and network conditions call for distinct routing protocols. From the perspective of the application, there are a number of ways to gather data from the environment. These include time-driven, event-driven, and query-driven approaches. The sensor nodes in a time-driven system communicate with base stations or gateways at regular intervals. When an event happens, sensor nodes in an event-driven system report the data they've acquired. In query driven techniques, the BS eventually sends a query to the nodes in order to seek their data [20].

IV RELATED WORKS

In [**21**], an approach to enhance network security against potential attacks from internet traffic intruders was presented. The proposed solution aimed to strike a balance between the imperative for protection and the constraints posed by available resources and trust factors. To achieve this, the research introduced a ranking-based route mutation mechanism that leverages the bafflement technique for selecting optimal routes for flows within the network. These routes are chosen based on diverse considerations, ensuring robust security at the base station level by incorporating factors such as route overlap, energy consumption, and link cost. Moreover, this strategy supports multiple

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

altered pathways that can confuse potential attackers, along with scrutiny algorithms tailored for fully centered WSNs. The technique involves strategically selecting multiple intruder sink nodes, which are designed to mislead attackers attempting to locate the true sink node. A suitable parameter is employed to account for the residual energy of neighboring nodes associated with the chosen intruder sink nodes. This parameter takes into consideration the expected additional communication cost within the corresponding region. Notably, this solution remains cost-effective and suitable for deployment in extensive sensor networks without imposing excessive expenses.

Another mechanism presented in [22] involves the implementation of a black-hole attack and introduces a corresponding prevention method for the AODV routing protocol within WSNs. The proposed prevention technique is centered on identifying the shortest paths between a non-compromised source and destination, as depicted in the diagram. It is important to note that both the source and destination nodes are presumed to be trustworthy and not compromised. Our approach involves incorporating the detection of malicious paths within the route-discovery phase of the AODV routing protocol.

A fuzzy-logic-based technique was proposed in [27] to tackle the issue of gray-hole attacks targeting WSNs nodes integrated into IoT systems. The IoT system incorporates WSN by establishing connectivity through a router to amass data. By leveraging the deployed sensors, the nodes can detect attacks within the IoT framework. Each node within the IoT network is systematically organized, serving various functions. This organization is underpinned by connecting users and clients to a central controller, the base station, facilitating IoT connectivity. The intricate architecture intrinsic to IoT renders it susceptible to gray-hole attacks. The sensor nodes situated within the WSN play a pivotal role in detecting attacks occurring within the IoT domain.

Routing protocols are pivotal in both WSN and IoT, effectively guiding the decision-making process for packet forwarding among nodes. Within the realms of IoT and WSN, two primary categories of routing protocols exist: proactive and reactive. Proactive routing protocols process network information, while reactive routing protocols manipulate the network's structure to facilitate efficient packet routing.

In [23], a system for detecting intruders in WSNs and responding with an intelligent mobile robot was described. This system employs an unsupervised neural network for intrusion detection, focusing on identifying changes over time using a Markov model. Once an intrusion is detected, a robot is dispatched to the affected area for further investigation. The reported results indicate an approximate detection rate of 85%.

Given that WSN nodes are often deployed in harsh and unattended environments, where attackers may compromise a subset of nodes, compromised sensor nodes can potentially transmit incorrect data to the central sink. To address this concern, a malicious-node-detection mechanism

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

is proposed in [29] for hierarchical WSNs, where nodes gather and share data with neighboring nodes. This mechanism utilizes a feed-forward ANN technique. The authors assert that their proposed approach effectively identifies malicious nodes, even when up to 25% of sensor nodes have been compromised.

In [24], the author placed a significant emphasis on addressing the challenge of detecting data anomalies in WSN. To tackle this issue, a convolutional neural network (CNN) model was meticulously crafted, leveraging the distinctive features of the marked mode and the deep neural network architecture to effectively identify anomalous data patterns. Throughout the study, the author introduced three innovative network models and conducts a comparative evaluation against a previously utilized CART (classification and regression trees) model. The assessment of these models was based on performance metrics such as detection accuracy (DA), true-positive rate (TPR), and precision (PRE). The experimental findings unequivocally demonstrate that the three models introduced in this research consistently outperform the CART model, with the M2 model exhibiting the highest level of performance.

A hybrid approach proposed in [25] combined the definition of fuzzy logic with the learning ability of neural networks to detect routing attacks in WSNs. The success of this solution depends on the quality and quantity of training data, the creation of fuzzy rules, the neural network architecture and the starting point. To ensure that the system effectively detects and mitigates attacks in a dynamic network environment, regular maintenance and development are required.

Table 3 summarizing the key aspects of clustering and routing protocols in Wireless Sensor Networks (WSNs)

Aspect	Fuzzy Logic-Based Clustering and Routing	Intelligent Computing Techniques	Integration of Fuzzy Logic with Intelligent Algorithms
Primary Focus	Optimizing network resource utilization through adaptive clustering	Enhancing efficiency in clustering and routing using intelligent methods	Combining fuzzy logic with intelligent algorithms to improve WSN performance
Example Protocols	LEACH, FUCA, E-FUCA	Enhanced GWO, CASIC-PSO, PDU-SLnO, IPSO-GWO, PSO-EEC, EBPSO	Fuzzy-based methods integrated with intelligent computing techniques
CH Selection Method	Fuzzy inference system based on residual energy,	Population-based methods (PSO, GWO)	Utilizes fuzzy logic for decision-making in

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

	distance, and neighbor count	considering multiple parameters	conjunction with intelligent algorithms
Data Transmission Approach	Multi-hop paths based on fuzzy clustering	Optimizing paths using various intelligent algorithms	Enhances routing decisions by integrating fuzzy logic with intelligent algorithms
Energy Management	Reduces energy consumption through dynamic adjustment of competition radius	Focuses on load balancing and fault tolerance	Aims to enhance energy efficiency and network lifespan through combined methods
Simulation Results	Improved performance through dynamic cluster formation	Proven effectiveness in maximizing energy efficiency and extending network lifetime	Validates improvements in clustering efficiency and energy consumption
Limitations Addressed	Uneven energy distribution and premature death of CHs	Convergence issues, local optima, and energy imbalance	Balances trade-offs between traditional methods and intelligent strategies

V CONCLSUION

The optimizing communication in Wireless Sensor Networks (WSNs) is crucial for enhancing network efficiency, energy conservation, and prolonging the network's lifespan. The review of clustering algorithms and routing protocols demonstrates that clustering plays a pivotal role in reducing energy consumption, minimizing communication overhead, and improving scalability in WSNs. Effective clustering algorithms such as LEACH, HEED, and DEEC optimize the selection of cluster heads and enhance intra-cluster communication, contributing to extended network longevity.Additionally, the integration of advanced routing protocols, including hierarchical, flat, and location-based approaches, enables more efficient data transmission. These protocols, especially when combined with energy-aware mechanisms, help in reducing latency, conserving energy, and improving the overall throughput of the network.By leveraging clustering and routing protocols, future WSN implementations can achieve more reliable communication, reduced power consumption, and better adaptability to changing network dynamics. However, ongoing challenges like load balancing, node mobility, and handling of large-scale networks still require further research to fully optimize communication in WSNs for diverse applications. The integration of machine learning, energy harvesting, and hybrid techniques holds promise for further advancements in this field.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

REFERENCES

1. Chijioke, W.; Jamal, A.A.; Mahiddin, N.A. Wireless Sensor Networks, Internet of Things, and Their Challenges. Int. J. Innov. Technol. Explor. Eng. 2019, 8, 2278–3075.
2. Kim, B.S.; Park, H.; Kim, K.H.; Godfrey, D.; Kim, K.I. A survey on real-time communications in wireless sensor networks. Wirel. Commun. Mob. Comput. 2017, 2017, 1864847.
3. Ali, A.; Ming, Y.; Chakraborty, S.; Iram, S. A comprehensive survey on real-time applications of WSN. Future Internet 2017, 9, 77.
4. Albaladejo, C.; Sánchez, P.; Iborra, A.; Soto, F.; López, J.A.; Torres, R. Wireless sensor networks for oceanographic monitoring: A systematic review. Sensors 2010, 10, 6948–6968.
5. Rashid, B.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. J. Netw. Comput. Appl. 2016, 60, 192–219.
6. Tandel, H.; Shah, R. A Survey Paper on Wireless Sensor Network. Int. J. Sci. Res. Dev. 2017, 5, 907–909
7. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. Comput. Netw. 2002, 38, 393–422.
8. Rawat, P.; Singh, K.D.; Chaouchi, H.; Bonnin, J.M. Wireless Sensor Networks: Recent developments and potential synergies. J. Supercomput. 2013, 68, 1–48.
9. Akyildiz, I.F.; Pompili, D.; Melodia, T. Challenges for efficient communication in underwater acoustic sensor networks. ACM Sigbed Rev. 2004, 1, 3–8.
10. Heinzelman, W.B.; Chandrakasan, A.P.; Balakrishnan, H. An application-specific protocol architecture for wireless micro sensor networks. IEEE Trans. Wirel. Commun. 2002, 1, 660–670.
11. Swetha, R.; Santhosh Amarnath, V.; Anitha Sofia, V.S. Wireless Sensor Network: A Survey. Int. J. Adv. Res.Comput. Commun. Eng. 2018, 7, 114–117.
12. Perrig, A.; Szewczyk, R.; Tygar, J.D.; Wen, V.; Culler, D.E. SPINS: Security protocols for sensor networks. Wirel. Netw. 2002, 8, 521–534.
13. Shi, E.; Perrig, A. Designing secure sensor networks. IEEE Wirel. Commun. 2004, 11, 38–43.
14. R.; Chen, Q.; Liu, Y.; Qin, W. Iot gateway: Bridging wireless sensor networks into internet of things. In Proceedings of the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 11–13 December 2010; pp. 347–352.
15. Kuo, Y.W.; Li, C.L.; Jhang, J.H.; Lin, S. Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications. IEEE Sens. J. 2018, 18, 5187–5197.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open access journal
Impact Factor: 8.3 www.ijesh.com ISSN: 2250 3552

16. Bhushan, S.; Pal, R.; Antoshchuk, S.G. Energy efficient clustering protocol for heterogeneous wireless sensor network: A hybrid approach using GA and K-means. In Proceedings of the 2018 IEEE Second International Conference on Data Stream Mining Processing (DSMP), Lviv, Ukraine, 21–25 August 2018; pp. 381–385.
17. Shi, Y.; Liu, E.; Zhou, G.; Shen, Z.; Yu, S. Bamboo shoot growth model based on the stochastic process and its application. Sci. Silvae Sin. 2013, 49, 89–93.
18. Kavitha, E.; Sowndeswari, S. Enhanced Security against Intruder Based on Bafflement Technique for Wireless Sensors Network Using Tracking Node with Scrutiny Algorithm. J. Data Acquis. Process. **2024**, 38, 1878.
19. Kalkha, H.; Satori, H.; Satori, K. Preventing Black Hole Attack in Wireless Sensor Network Using HMM. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **2019**, 10, 293–299.
20. Ye, Q.; Wang, Y.; Xi, M.; Tang, Y. Recognition of grey hole attacks in wireless sensor networks using fuzzy logic in IoT. Trans. Emerg. Telecommun. Technol. **2024**, 31, 3873.
21. Cauteruccio, F.; Fortino, G.; Guerrieri, A.; Liotta, A.; Mocanu, D.C.; Perra, C.; Terracina, G.; Vega, M.T. Short-long term anomaly detection in wireless sensor networks based on machine learning and multiparameter zed edit distance. Inf. Fusion **2019**, 52, 13–30.
22. Shen, X.; Zhu, C.; Zang, Y.; Niu, S. A Method for Detecting Abnormal Data of Network Nodes Based on Convolutional Neural Network. J. Comput. **2022**, 33, 49–58
23. Alenezi, M.; Reed, M.J. Denial of service detection through TCP congestion window analysis. In Proceedings of the World Congress on Internet Security (WorldCIS-2013), London, UK, 9–12 December 2013; pp. 145–150.
24. Kanev, A.; Nasteka, A.; Bessonova, C.; Nevmerzhitsky, D.; Silaev, A.; Efremov, A.; Nikiforova, K. Anomaly detection in wireless sensor network of the ‘smart home’ system. In Proceedings of the 20th Conference of open innovations association (FRUCT), St. Petersburg, Russia, 3–7 April 2017; IEEE: Piscataway, NJ, USA, 2017.
25. Ezhilarasi, M.; Gnanaprasanambikai, L.; Kousalya, A.; Shanmugapriya, M. A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. Soft Comput. **2023**, 27, 4157–4168.