Resilient and Adaptive Secure Routing Protocol for Wireless Sensor Networks Using a Grey Wolf Optimizer and Lightning Search Algorithm

G. Aravindh[1*], and Capt. Dr.K.P. Sridhar[2]

[1*]Research Scholar, Department of ECE, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India. aravindhvlsi@gmail.com, https://orcid.org/0000-0003-3831-5414

[2]Professor, Department of ECE, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India. sridhar.kp@kahedu.edu.in, https://orcid.org/0000-0001-9377-7182

Received: July 14, 2024; Revised: August 22, 2024; Accepted: September 25, 2024; Published: November 30, 2024

Abstract

The ability of Wireless Sensor Networks (WSNs) to efficiently monitor and collect data from difficult and distant places has made them a notable technical solution for a variety of applications. It is crucial to optimize energy usage and secure data integrity in order to put these technologies to reality with the Internet of Things (IoT). Maintaining a balance between energy economy, flexibility to changing network circumstances, and security is a common difficulty for contemporary routing systems. Because of this, the performance of these protocols drops and they become vulnerable. Specifically, for WSNs, this research presents HGL-ASRP, a state-of-the-art Resilient and Adaptive Secure Routing Protocol. By integrating the Quantum Assisted Grey Wolf Optimizer (GWO) with the Lightning Search Algorithm (LSA), this protocol overcomes the challenges faced by previous routing protocols in the Internet of Things (IoT) setting. Hybrid GWO takes cues from the social behavior of grey wolves and uses them to solve optimization problems very well. As a result of this hybrid GWO and hypercube sampling, grey wolves can only go to a better area to live. With hypercube sampling, the HGL-ASRP method performs better in a number of areas, including speed (90.9 kbps), end-to-end delay (88.8 ms), packet delivery ratio (91.2%), energy efficiency (92.09%), network lifetime (163.63 hours), and security (87.59%). The HGL-ASRP system ensures continuous data transmission even in demanding environments by successfully managing node failures and changing topologies.

Keywords: Wireless Sensor Network, Routing, Grey Wolf, Energy Efficiency, Internet of Things.

1 Introduction to Wireless Sensor Networks

Enabling wireless services via environmental sensing, Wireless Sensor Networks (WSNs) (Singh et al., 2021) are a key component. While security is a major concern with WSNs, power consumption becomes an issue. Energy efficiency in routing protocols is an important issue right now, and a lot of people are working to find solutions. There are two primary types of WSNs: organized networks and unstructured networks. An unstructured WSN is an ad hoc network with a high density of sensor nodes (Singh & Saini, 2022).

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 331-346.
DOI: *10.58346/JISIS.2024.I4.020*

*Corresponding author: Research Scholar, Department of ECE, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India.

The energy consumption and longevity of the network are both improved by a hierarchical routing strategy that uses clustering Daanoune et al., 2021; Jawad et al., 2022). The goal of this protocol is to evenly share the network's energy usage across all nodes while keeping transmission distance to a minimum. Because of this, we may conclude that the technique is very efficient and effective. A clustering protocol is required to partition the area of the sensing operation into clusters. In order to improve communication inside the cluster, each group selects a Cluster Head (CH) (Ramya & Brindha, 2022). After the fusion process, the data collected by the nodes in the cluster are sent to the BS (Gao et al., 2022). Choosing CHs optimally and making sure the cluster structure is distributed appropriately are two of the most important aspects of clustering procedures. Even though there are a lot of issues with clustering-based routing protocols, choose the right CH is often considered the most important factor.

Recently, WSNs have encountered heightened insecurity due to targeted attacks by malicious actors on multiple network nodes in the presence of the Internet of Things (IoT) (Ávila et al., 2022). The IoT is a burgeoning paradigm that establishes a plethora of intelligent applications. The IoT is commonly combined with WSN to be utilized in various domains such as smart cities, healthcare (Keerthika & Shanmugapriya, 2021), transportation, among other service. Integrating various systems also presents challenges like scalability, compatibility, energy efficiency, and security. Certain types of attacks at the routing level are called black hole, Sybil, spoofing, and Denial of Service (DoS) attacks (Keerthika & Shanmugapriya, 2021). Among the various security challenges, one that holds significant importance is the DoS attack. Numerous researchers are developing a novel secure routing protocol aimed at enhancing the security of WSNs (Sreevidya & Supriya, 2024). This study introduces a novel routing algorithm that prioritizes energy efficiency by effectively detecting and mitigating security attacks. The issue of energy consumption in WSNs arises when nodes engage in malicious activities. Hence, it has been determined that energy conservation in sensor nodes can be achieved by preventing malicious activities (Naeem et al., 2021). To ensure secure communication in IoT, it is imperative to establish a specific pathway that can be authenticated by computing the nodes' trustworthiness Abbas et al., 2021; Prakash & Prakash, 2023).

2 Related Works

One possible approach to developing intelligent and sustainable Internet of Things (IoT) applications was proposed by Patel et al. in their paper on ECARP (Patel et al., 2021). The ECARP system optimizes the network's performance using a hybrid approach that combines energy awareness and collision avoidance algorithms.

It was (Nabavi et al., 2021) who first proposed the Multiobjective Greedy-based Routing Protocol (MGRP) for WSNs. Energy usage and latency are two of the many goals that the MGRP strives to optimize. Significant results were obtained in the MGRP simulations, with a 20% reduction in energy usage and a 15% decrease in time as compared to other routing protocols. These results demonstrate that MGRP works well with WSNs.

Using a multi-hop technique based on re-clustering, Rezaeipanah et al., (2021) proposed EAHRP, an Energy-Aware Hybrid Routing Protocol. Improving the endurance of network operations via energy optimization is the main goal of the EAHRP. With a 25% extension over conventional protocols, EAHRP's testing findings show a considerable improvement in the total time of network operation. Based on these results, EAHRP is clearly a workable strategy for boosting WSN efficiency.

Using Ant Colony Optimization (ACO) methods, Moussa et al., (2023) developed a WSN routing protocol. Making forest fire detection easier is the primary goal of this protocol (Elfarra et al., 2023; Suvarna, & Bharadwaj, 2024). The methodology being discussed has an emphasis on maximizing efficiency in energy usage and guaranteeing consistent performance in challenging environments. The simulation results showed that the ACO-based protocol outperformed the state-of-the-art approaches. It improved energy efficiency by 40% and provided a more reliable communication channel for fire monitoring in forests.

To address the issue of energy-undomed WSNs, Liang et al., developed the ACRT protocol (Liang et al., 2021). To make the most efficient use of its resources, the ACRT system uses adaptive routing techniques that are constantly modified in reaction to changing energy levels. As compared to traditional systems, the ACRT improved network performance by reducing energy usage by 25% on average. This result demonstrates the effectiveness of ACRT in situations with constrained energy supplies.

To improve the security of WSNs, Kumar et al. suggested using TLR-CBDBE, which stands for Trust-Aware Localized Routing and Class-Based Dynamic Blockchain Encryption Scheme (Hema Kumar et al., 2021). To guarantee data transmission security, the suggested protocol combines trust-aware routing with blockchain-based encryption. In order to protect sensitive information and reduce the impact of assaults, the testing findings show that TLR-CBDBE is very secure. Using TLR-CBDBE greatly improves the safety of WSNs in general.

3 Proposed Energy-efficient and Secured Routing Protocol

The proposed framework presents a new method named HGL-ASRP that analyzes nodes, packets, and routes to comprehend the network's dynamic properties and choose the best path. This method guarantees safe and efficient data transfer by removing potential invaders. A secure and energy-efficient routing solution in WSNs is offered by the recommended structure, as shown in Figure 1. The Internet of Things (IoT) network is built and launched in a continuous environment and consists of a set of interconnected nodes.

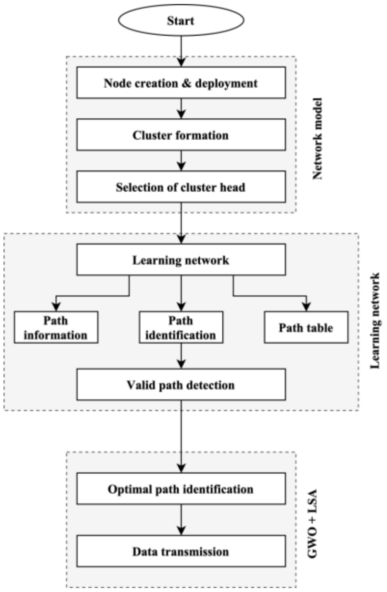

Figure 1: Workflow of the Proposed HGL-ASRP

Groups develop once the nodes have been deployed. Groups are physically formed. The geographical collection of clusters is achieved through the equal classification of spatial regions. The suggested approach involves the formation of three hierarchical clusters, wherein the area place is separated into three equal sections.

Figure 2 illustrates the flowchart of the HGL-ASRP integrated with GWO and LSA. The network is set up, and all nodes are chosen randomly in an interconnected connection-based system. The values of parameters such as the total amount of dynamic sensor nodes, initial energy allocation for each IoT node, the size of packets, and acknowledgment size are initialized. The nodes are selected rapidly from the provided network, and all potential paths from the first/initial node to the desired node are determined. The HGL-ASRP utilizes the path table to determine the validity of a given path. The information will be incorporated into the IoT path table if deemed valid. The GWO algorithm examines the node, path, and packet data stored in the route table and selects the most suitable route. The messages are transmitted along this chosen path in the IoT network.

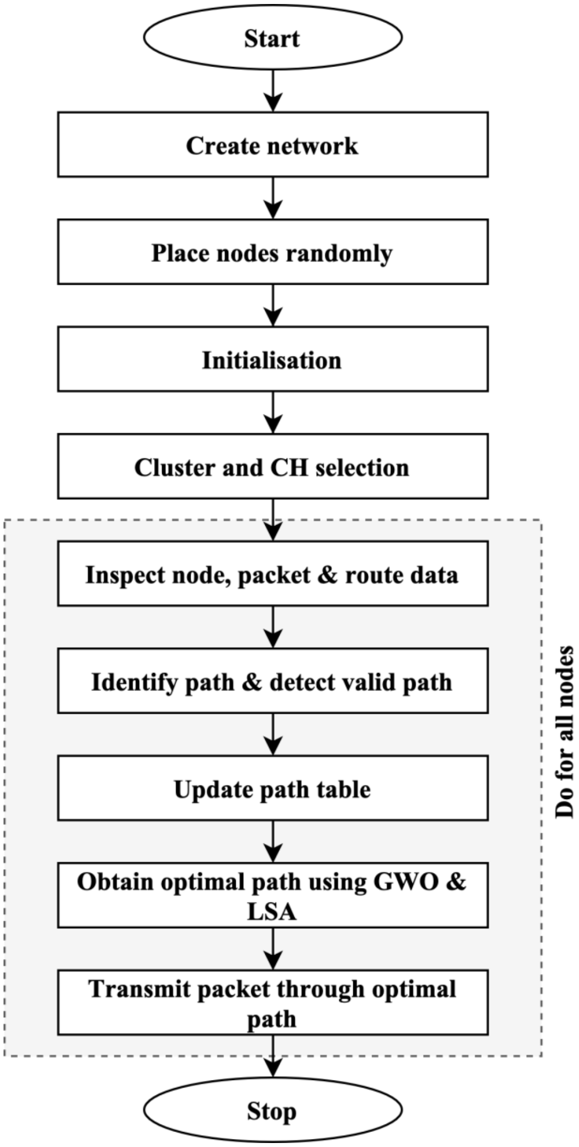
Start
Create network
Place nodes randomly
Initialisation
Cluster and CH selection
Inspect node, packet & route data
Identify path & detect valid path
Update path table
Obtain optimal path using GWO & LSA
Transmit packet through optimal path
Do for all nodes
Stop

Figure 2: Workflow of the Secured Routing Process

3.1. Quantum Assisted Grey Wolf Optimizer

The principle of GWO is based on the dynamics of grey wolf hunting behavior and their social structure [23]. The optimal solution is determined by using grey wolves engaging in prey hunting. In this context, "prey" refers to the optimal solution.

The energy consumption model for a sensor node with IoT is illustrated as follows:

Energy consumption for transmission of the messagee_T is expressed in Equation (1).

$$e_T = \left(a_1 + a_2 D^k\right) M \tag{1}$$

Energy consumption for the reception of the messagee_R is expressed in Equation (2).

$$e_R = a_3 M \tag{2}$$

Energy consumption for the idle state of WSNe_I is expressed in Equation (3).

$$e_I = a_4 I_t P(M) \tag{3}$$

The variable D reflects the communication distance, k indicates the path loss exponent, and M symbolizes the message size. I is used to indicate the idle time of IoT device. The symbol $P(M)$ is utilized to predict the message-analyzing rate of the detector. The values of a_1, a_2, a_3 and a_4 are system-dependent ones.

3.1.1. Prey Encircling

The act of hunting involves initiating the process of surrounding the targeted prey. The optimal solution is found by surrounding the grey wolves, as outlined in Equations (4) and (5).

$$E = \left|DY_{prey}(x) - Y_{prey}(x)\right| \tag{4}$$

$$Y_{wolf}(x+1) = Y_{prey}(t) - AE \tag{5}$$

The variable "x" represents the current repetition number in IoT. The vectors "A" and "D" represent the coefficients, while "$wolf$" and "Y" represent the vectors of the wolf's location and the prey's location, respectively. The determination of the vectors of coefficients $A \, and \, D$ is accomplished by Equations (6) and (7).

$$A = 2ar_1 - v \tag{6}$$

$$D = 2r_2 \tag{7}$$

The vector values v exhibit a successive decline from 2 to 0. The vectors r_1 and r_2 are random and subject to the constraint (a) of being within the interval [0, 1].

3.1.2. Prey Hunting

In an actual situation, the precise whereabouts of the prey are determined, whereas, in an optimization issue, the best approach remains unknown. This process guarantees the attainment of optimal solutions. The determination of the wolves' location update is characterized by Equation (8).

$$Y_{wolf}(x+1) = \frac{Y_1+Y_2+Y_3}{3} \tag{8}$$

$Y_1, Y_2, and \; Y_3$ are estimated using Equations (9) to (12).

$$Y_1 = Y_1 - A_1(D_a) \tag{9a}$$

$$D_a = \left|C_1 Y_a - Y_{wolf}\right| \tag{9b}$$

$$Y_2 = Y_b - A_2(D_b) \tag{10a}$$

$$D_b = \left|C_1 Y_b - Y_{wolf}\right| \tag{10b}$$

$$Y_3 = Y_c - A_3(D_c) \tag{11a}$$

$$D_c = \left|C_1 Y_c - Y_{wolf}\right| \tag{12}$$

Equations 9, 10, and 11 analyze the precise position of the prey, which is regarded as the optimal solution. The wolf location is expressed Y_{wolf}, scaling coefficients are expressed $A_1, A_2, and\ A_3$, a distance of prey is expressed $D_a, D_b, and\ D_c$. The location factors are expressed $C_1, C_2\ and\ C_3$, and the prey positions are expressed $Y_a, Y_b\ and\ Y_c$. The mean place of the prey is calculated, serving as the target place for the wolf to advance towards to capture the prey in IoT.

3.1.3. Prey Attacking

To achieve this objective, the fitness function is calculated. The derivation is as follows:

(i) The residual energy of the CH is a crucial factor in the process of transmitting packets. During this process, the relay node receives and gathers data before forwarding it to the sink node. Therefore, having a relay node with a higher energy level for the hop is advantageous. The calculation is performed by Equation (13).

$$f_1 = \sum_{x=0}^{m-1} s_{CH} \tag{13}$$

The energy required for transmission is expressed as s_{CH}, and m messages are sent.

(ii) The measurement of the spatial separation between the sensor node and the sink node is denoted as the separation. The Euclidean separation determines the spatial separation between the CH and the relay node and between the CH and their respective base station. A route is determined when the break to the sink point is at its lowest point. The spatial separation is expressed in Equation (14).

$$f_2 = \frac{1}{\sum_{x=0}^{m-1} d(CH,R) + d(CH,S)} \tag{14}$$

The transmitter (S) and the receiver (R) distance are expressed as $d(CH,S), and\ d(CH,R)$.

(iii) The level of CH is calculated by deciding the number of CH members contained by the next transmit node. If the relay node possesses a limited number of cluster head members, it will reduce energy consumption during the transmission and reception of data. A channel with low channel hardness is considered the preferred data transmission option. The concept is articulated by Equation (15).

$$f_3 = \frac{1}{\sum_{x=0}^{m-1} y_x} \tag{15}$$

The channel hardness is expressed y_x.

The weight value is determined using three measurements which is mathematically defined by Equation (16).

$$F = k_1(f_1) + k_2(f_2) + k_3(f_3) \tag{16}$$

The fitness functions are expressed as $f_1, f_2\ and\ f_3$, and the weight factors are expressed as $k_1, k_2\ and\ k_3$. The location of each prey is continually revised, with the less bright prey being drawn closer to brighter ones. The HS approach, which guarantees space-filling qualities and reduces calculation scale, is based on the scalar discriminant function since this method's calculation scale is far enormous. Here is the equation (17) for its scalar discriminant function.

$$\partial_p(Y) = \left(\sum_{j=1}^{n} I_j d_j^{-p}\right)^{1/p} \tag{17}$$

where p is a positive integer indicating the mode norm of the space and $d_j, j = 1,2,3 \ldots\ldots n$ is the distance between all possible combinations of two points in the sampling matrix $Y, j = 1,2,3 \ldots\ldots n$ is the number of pairs of points in the sampling matrix $Y$with distance d_j. Figure 3 shows the various distributions of the random procedure and the HS method's initializations when generating 100 grey wolves, those between [0, 1] in two dimensions.

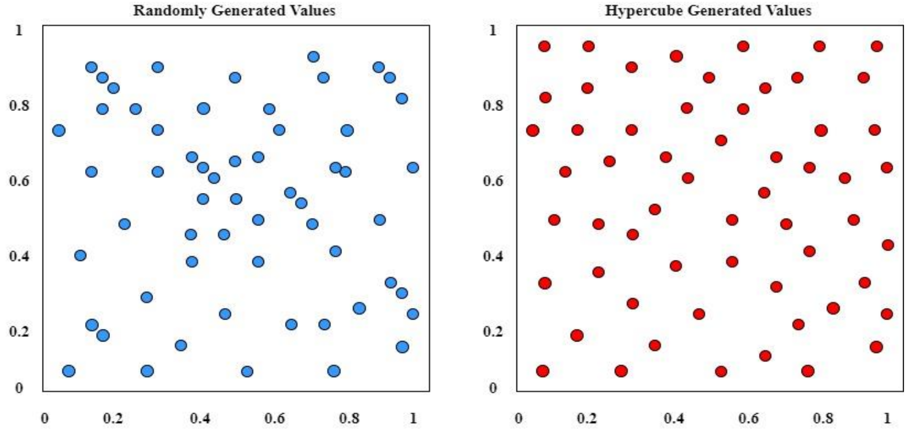

Figure 3: Hybercube Generated Values

The wolves in the Quantum Assisted GREY WOLF OPTIMIZER are completely skewed toward the locations of the α and δ wolves, and therefore are not particularly effective at emerging from local optimums. Therefore, an equation for updating positions to perform extended research is suggested. The equation (18, 19) is the shown in below.

$$Y(d+1)' = \frac{(Y_1+Y_2+Y_3)}{3} + Y_N(d) - r.Y_\vartheta(d) \qquad (18)$$

$$Y_N(d) = \frac{1}{M}\sum_{j=1}^{M} Y_j(d) \qquad (19)$$

where $Y_N(d)$ is the average position vector of all grey wolves at iteration d, and r is a random vector between 0 and 1.

3.2. Lightning Search Algorithm

The natural occurrence of lightning has influenced the advancement of the novel metaheuristic method referred to as LSA. The primary principle underlying this approach involves the extension of the hypothesis, which is interconnected with the process of step leader transmission in IoT. The LSA employs projectiles, which consist of fast-moving particles that navigate the search space in the shape of a binary tree framework associated with a step leader.

- **Transition Projectiles**

The initial group of step leaders is comprised of these projectiles. Producing these projectiles involves randomly selected numbers from the standard consistent distribution of probabilities $(x \; and \; y)$. The likelihood density function $(f(i))$ of the distribution is defined by Equation (20).

$$f(i) = \begin{cases} \frac{1}{x+1} & x < i < y \\ 0 & else \end{cases} \qquad (20)$$

- **Space Projectiles**

The projectiles undergo updates and evolutionary changes, resulting in the emergence of a leader among them. The updating system is implemented using Equation (21).

$$p_y^s = p_x^s \pm f(D) \tag{21}$$

The equation introduces the new place projectile as p_y^s, the old place projectile as p_x^s, and a function indicated as $f(D)$ that generates random numbers from exponential dissemination for IoT. The likelihood density function of the exponential spectrum is given by Equation (22):

$$f(i) = \begin{cases} \frac{\exp\left(-\frac{i}{\beta}\right)}{\beta} & i > 0 \\ 0 & else \end{cases} \tag{22}$$

The presumption is that the symbol β represents the distance D among the lead projectile p_L^x and the p_x^s, as denoted in Equation (23).

$$D = |p_L^x - p_x^s| \tag{23}$$

An algorithm called LSA is proposed in this study to solve the constraints and difficulties. This relies on the natural phenomena of lightning and uses the idea of fast particles designated fighters, which led to the development and production of three different kinds of aircraft. The first stage include the leader of the population. Stage two involves space projectiles that aspire to become pilots, and stage three consists of a lead shell dependent on the commander's finest missile. Exploration was planned with the projectile's exponential and random fences in mind, which aligns with the leader's counsel and is based on opposition theory. Specifically, the suggested technique was tested using LSA on a dataset of 24 functions with varying properties.

3.3. Proposed Hybrid Algorithm

The HGL-ASRP method considers LSA as the principal procedure. The introduction of the SA mechanism incorporates the use of LSA in the crossover and mutation activities to optimize the population. A novel crossover operation involves the iterative selection of a specific number of individuals, utilizing a managed pool based on the probability of a parent chromosome (P_{ch}) and the occurrence of a crossover event. A random two-point crossover is performed on two individuals within the population, precisely two male individuals from the bank of IoT. This ensures that both individuals have an equal number of sub-units.

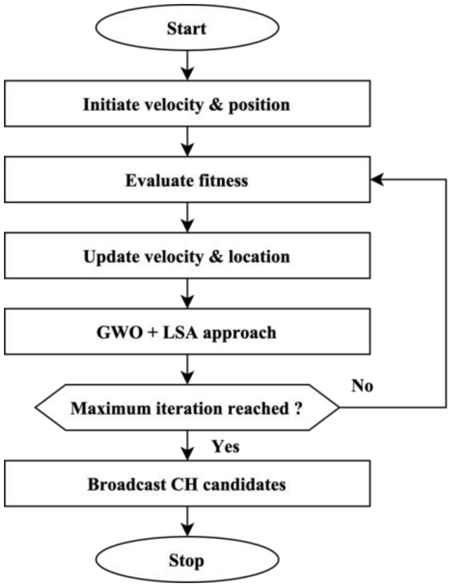
Start
Initiate velocity & position
Evaluate fitness
Update velocity & location
GWO + LSA approach
Maximum iteration reached ?
No
Yes
Broadcast CH candidates
Stop

Figure 4: Flowchart of the HGL-ASRP for Route Selection

The flowchart of the route selection process based on energy and security is shown in Figure 4. The ability for rapid convergence is one of GWO's pros. However, there are a few drawbacks to this strategy as well. For example, it can get easily captured in the local optima of IoT nodes and experience premature convergence. The high convergence rate of conventional LSA is one of its benefits. There are certain limits to the approach that need to be addressed. For example, it cannot be particularly effective at solving optimization problems with many different aspects, it converges too quickly, and it can get stuck in local optima. Someone has proposed using an HGL-ASRP to make LSA search more effective.

3.4. Secure Routing Algorithm

This study introduces an innovative protocol named the HGL-ASRP routing procedure, which aims to enhance the security of the conventional Dynamic Source Routing (DSR) procedure by implementing an adaptive local surveillance technique in IoT. The utilization of adaptive local monitoring is a highly effective technique for the detection of misrouting attacks. A misrouting assault occurs when a malevolent node is present between the source and location in a network. In this context, a discovered path type is employed for discovery and maintenance processes. The purpose of this mechanism is to store and retrieve the built-up IoT-based path data within the dynamic source route procedure.

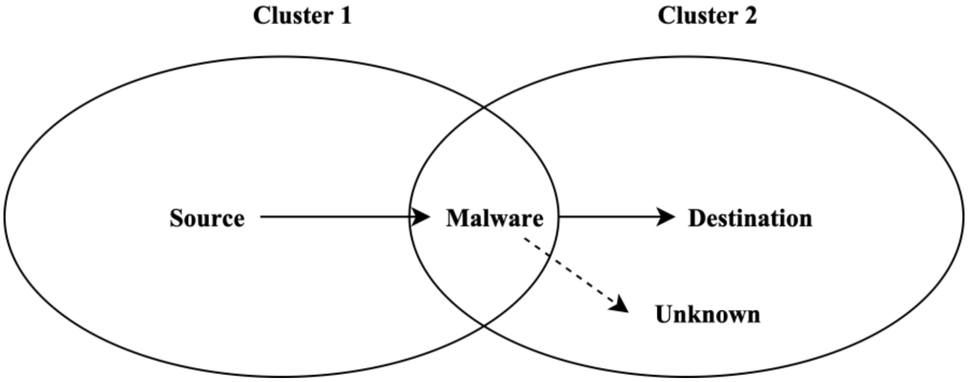

Figure 5: Route Selection and Malware Identification

Figure 5 illustrates an instance of a misrouting assault. When the source node relays the packet, node M gets it and forwards it to an unknown intermediate node instead of delivering it directly to the intended destination. The phenomenon referred to is commonly known as a misrouting assault. Using IoT guard nodes in Adaptive Local Monitoring facilitates the determination of adjacent node conduct. Guard nodes must store supplementary data about the routing path acquired during establishing the route. The data structure employed by each guard node comprises several components, including immediate source, immediate location, original location, final location, packet id, packet knowledge, residual energy, and time stamp. The time stamp denotes the designated time at which the primary source is required to transmit the packet, failing which the malicious count will be increased by one.

4 Simulation Analysis and Outcomes

The suggested HGL-ASRP system is employed to augment security and energy efficiency within a proficient cluster formation. The experiments utilized NS-3.38 on a 32-bit processor running Ubuntu 22.04. In a networked environment, the number of sensor nodes typically ranges from 100 to 1000, and these nodes are deployed randomly within a 1000 m × 1000 m area. The simulation tests will be conducted multiple times to ensure the results' stability and validity across varying rounds which is shown in Table 1. The simulation is conducted iteratively until sufficiently optimized results are obtained. The NS3.38 framework utilizes the NetAim visual features to facilitate the visualization of node distribution within a 2D variable space. After conducting multiple iterations, the system successfully identified a route that effectively reduces the average data transfer time without incurring additional overhead across the entire parameter space. At the outset, all nodes are assumed to have an equivalent energy level of 10J. The nodes were permitted to transition from a velocity of 10 m/s to a rate of 50 m/s to conduct the tests.

Dataset Description

WSN Technology has enabled tiny, low-cost sensors to sense diverse physical and environmental variables, interpret data, and communicate wirelessly. Sensor nodes in WSN have restricted transmission range, computation, storage, and energy. Wireless sensors have shown that the Triple Umpiring System (TUS) functions better. Clustering extends WSN lifespan. We have added SNR-based dynamic clustering to Ad hoc Demand Distance Vector Routing (AODV) in this research. Efficient and Secure Routing Protocol for WSNs through SNR-based Dynamic Clustering Systems (ESRPSDC) partitions nodes into clusters. It selects a Cluster Head (CH) based on energy, and Non-Cluster Head (NCH) nodes connect with a specific CH based on SNR values.

By optimizing sending actions, minimizing power use, decreasing safety risks, and improving the accuracy of data transfer, the suggested HGL-ASRP is an essential element of creative protocol designs that help ensure the security and stability of WSN installation in the long term.

Table 1: Simulation Parameters and their Values

S.no	Simulation parameters	Values
1	Number of sensor nodes	100 to 1000
2	NetAim visual features	NS3.38 framework with 2D space
3	Transmission velocity	10m/s to 50 m/s
4	Nodes Energy level	10J
5	Network deployment	1000m x 1000m area
6	Data packet size	512 bytes

The mean throughput (kilobits per second) for all methods is shown in Figure 6. The following are the values for various metrics: ECARP: 794.55, MGRP: 850.69, EAHRP: 821.44, ACO: 791.61, ACRT: 812.39, TLR-CBDBE: 839.69, MO-ACOSRP: 865.86, IPF: 836.55, TSIOP: 817.62, TASRP: 852.59, IFRAOD: 866.05, QoS-TBRA: 836.26, HGL-ASRP: 890.06. The HGL-ASRP demonstrates a mean enhancement of 11.8% in throughput compared to alternative methodologies. This possesses a superior capability to achieve elevated IoT-based data transmission rates. The increase in the number of nodes results in a decrease in throughput for all routing protocols. This can be attributed to the heightened network congestion and communication overhead. The HGL-ASRP continues to exhibit the most substantial throughput, thereby highlighting its efficacy in sustaining superior performance, even when dealing with larger network sizes.

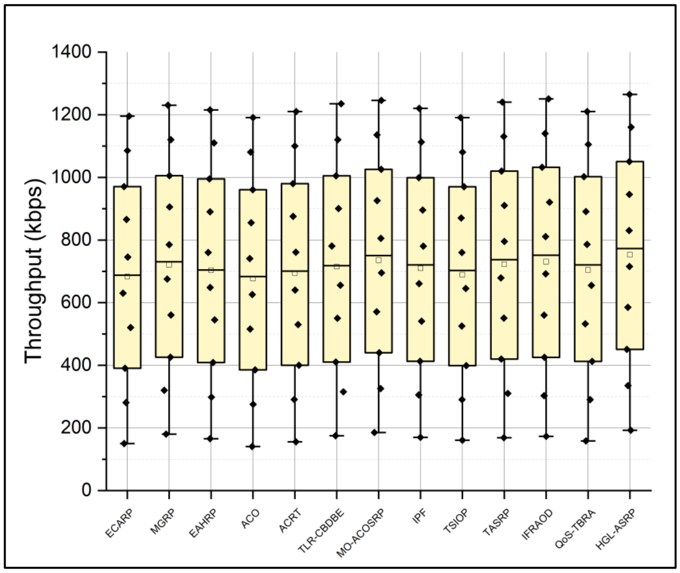

Figure 6: Throughput Analysis of the Different Routing Methods

This parameter's value represents the sum of all packets the destination receives in a specific time frame. This measure may be used to assess how well a routing mechanism works. The Equation (24) is below.

$$Throughput = \frac{File\ size}{Transmission\ time(bps)} \tag{24}$$

The mean value of the end-to-end delay (in milliseconds) for all methods is expressed in Figure 7. The following are the academic performance metrics for the respective evaluation criteria: ECARP (21.67), MGRP (22.37), EAHRP (20.84), ACO (22.08), ACRT (22.09), TLR-CBDBE (23.53), MO-ACOSRP (22.65), IPF (22.09), TSIOP (23.07), TASRP (22.13), IFRAOD (22.47), QoS-TBRA (22.10), and HGL-ASRP (21.18). The HGL-ASRP demonstrates a mean enhancement of 2.75% in end-to-end delay compared to alternative approaches. The HGL-ASRP can decrease the duration required for data transmission across the IoT network. The number of nodes in a network leads to a corresponding increase in the end-to-end delay for all routing protocols.

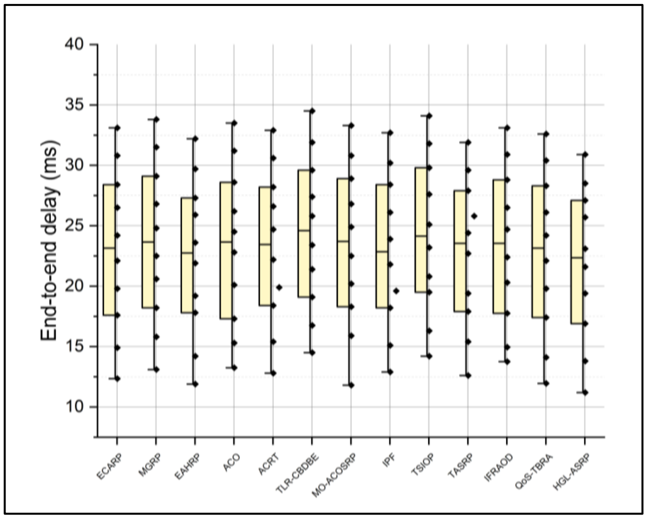

Figure 7: End-to-end Delay Analysis of the Different Routing Methods

The mean Packet Delivery Ratio (%) for all methods is plotted in Figure 8. The ECARP score is 93.89, the MGRP score is 94.49, the EAHRP score is 93.45, the ACO score is 93.20, the ACRT score is 93.75, the TLR-CBDBE score is 94.04, the MO-ACOSRP score is 94.25, the IPF score is 93.91, the TSIOP score is 93.68, the TASRP score is 93.99, the IFRAOD score is 93.52, and the QoS-TBRA score is 93.54. The HGL-ASRP value is recorded as 94.07. The HGL-ASRP exhibits a mean enhancement of 0.18% in the Packet Delivery Ratio compared to alternative approaches. The HGL-ASRP displays slightly superior performance in guaranteeing the successful delivery of packets. As the quantity of nodes in an IoT network expands, there is a tendency for the Packet Delivery Ratio to decline across all routing protocols. This can be attributed to heightened network congestion and the potential occurrence of packet losses. HGL-ASRP demonstrates a comparatively elevated delivery ratio, thus highlighting its efficacy in managing larger network sizes and enhancing packet delivery.

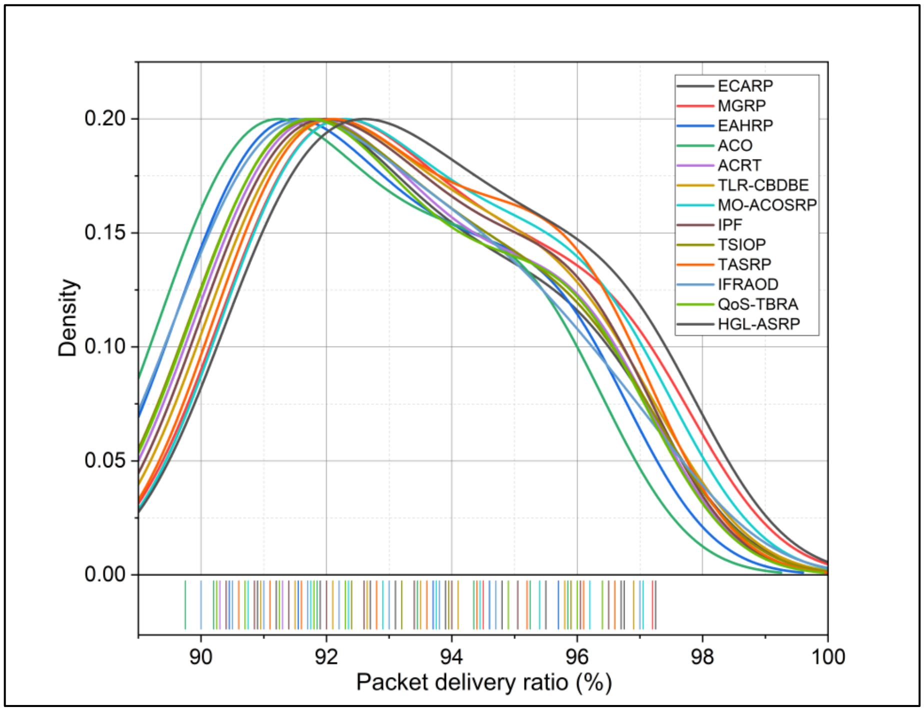

Figure 8: Packet Delivery Ratio Analysis of the different Routing Methods

The mean energy efficiency percentage for all methods is plotted in Figure 9. The following metrics were obtained: ECARP of 87.92, MGRP of 89.59, EAHRP of 88.74, ACO of 86.46, ACRT of 88.39, TLR-CBDBE of 89.53, MO-ACOSRP of 91.03, IPF of 89.14, TSIOP of 88.62, TASRP of 89.44, IFRAOD of 90.01, and QoS-TBRA of 89.34. The HGL-ASRP value is 92.09. The HGL-ASRP demonstrates a mean enhancement of 4.81% in Energy Efficiency compared to alternative methodologies. The HGL-ASRP exhibits superior efficacy in optimizing the utilization of energy resources. The outcomes show variation as the quantity of nodes escalates, primarily attributable to IoT network congestion and heightened energy consumption in the upkeep of communication links. The HGL-ASRP enhances energy efficiency by optimizing routing paths and reducing unnecessary energy consumption.

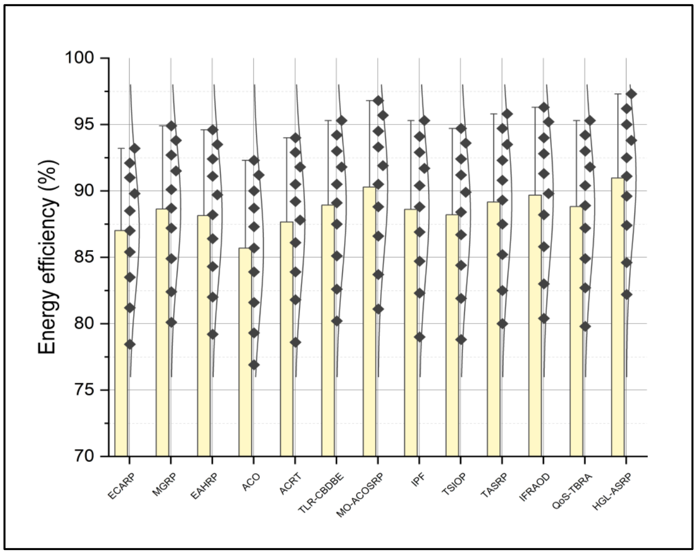

Figure 9: Energy Efficiency Analysis of the different Routing Methods

The mean duration of network lifetime (in hours) for all methods is plotted in Figure 10. The following are the abbreviations and corresponding values for various metrics: ECARP (155.67), MGRP (166.28), EAHRP (147.39), ACO (131.33), ACRT (146.96), TLR-CBDBE (162.69), MO-ACOSRP (167.57), IPF (147.81), TSIOP (137.42), TASRP (152.21), IFRAOD (156.06), QoS-TBRA (140.33), HGL-ASRP (163.63). The HGL-ASRP exhibits a mean enhancement of 4.98% in Network Lifetime when contrasted with alternative approaches. The HGL-ASRP can extend the network functionality duration before the energy depletion in nodes. The observed outcomes exhibit variation as the number of nodes is augmented due to the heightened energy consumption associated with increased nodes. This accelerated depletion of energy resources ultimately results in a reduction of the overall IoT network lifetime. The HGL-ASRP demonstrates superior energy management and routing capabilities, leading to a prolonged IoT network lifespan, even when dealing with more nodes.

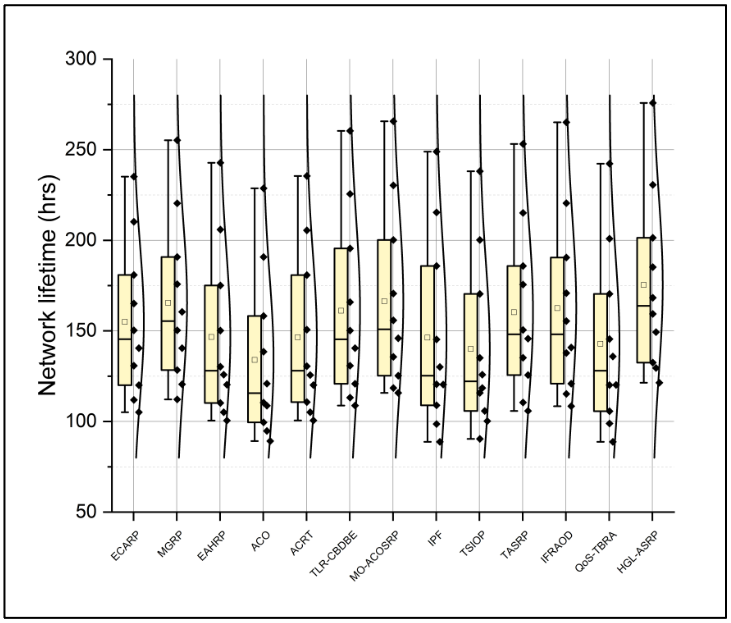

Figure 10: Network Lifetime Analysis of the Different Routing Methods

The mean security percentage for all methods is shown in Figure 11. The following are the academic performance indicators for the individual in question: ECARP (85.98), MGRP (87.43), EAHRP (84.39), ACO (81.76), ACRT (84.87), TLR-CBDBE (86.60), MO-ACOSRP (88.38), IPF (84.12), TSIOP (82.77), TASRP (85.28), IFRAOD (86.09), QoS-TBRA (83.74), and HGL-ASRP (87.59). The HGL-ASRP demonstrates a mean enhancement of 1.16% in Security compared to alternative methods. This possesses marginally stronger security measures to safeguard data transmission and nodes from attacks.

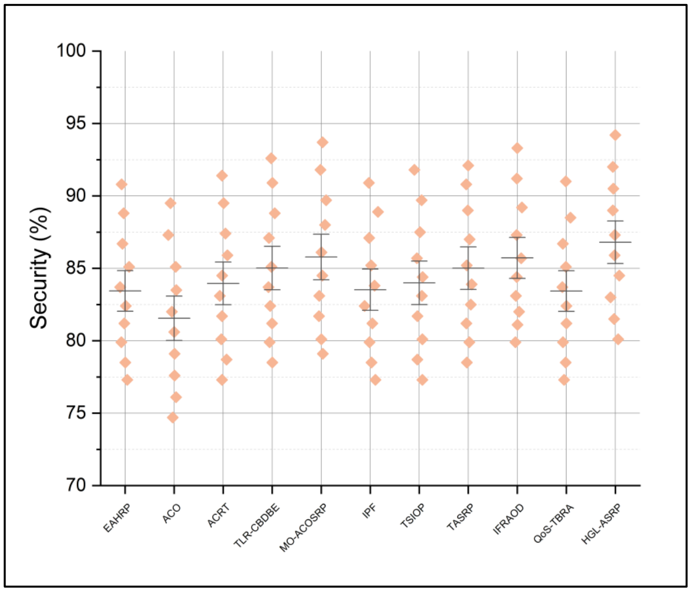

Figure 11: Security Analysis of the Different Routing Methods

The HGL-ASRP method exhibits notable advantages in terms of enhanced performance metrics. These include a higher throughput of 90.9 kilobits per second, a lower end-to-end delay of 88.8 milliseconds, an improved packet delivery ratio of 91.2%, increased energy efficiency of 92.09%, an extended network lifetime of 163.63 hours, and enhanced security with a rating of 87.59%. This study's findings underscore the efficacy of HGL-ASRP in attaining enhanced performance, energy utilization, and security for WSNs.

5 Conclusion and Future Studies

WSNs depict networks comprising small sensor nodes responsible for collecting and transmitting data from the surrounding environment. The current routing protocols employed in WSNs frequently need help achieving a satisfactory equilibrium between ensuring secure data transmission and maintaining energy-efficient operation with IoT. This often results in suboptimal network performance. The hybrid HGL-ASRP demonstrates notable improvements in various performance metrics. These include achieving a higher throughput of 90.9 kbps, a lower end-to-end delay of 88.8 ms, an improved packet delivery ratio of 91.2%, increased energy efficiency of 92.09%, an extended network lifetime of 163.63 hours, and enhanced security with a rating of 87.59%. The HGL-ASRP exhibits an average enhancement of 1.16% in security, 4.81% in energy efficiency, and 2.75% in end-to-end delay compared to alternative approaches. This outcome contributes to establishing more resilient data transmission and improved energy utilization in IoT. WSNs encounter various obstacles while addressing node mobility, dynamic network topologies, and resource limitations. The development of resilient and adaptable routing mechanisms becomes imperative. Future research is warranted to examine the potential of machine learning-based methodologies, integration of blockchain technology, and the utilization of energy harvesting techniques to augment the performance, security, and energy efficiency of WSNs.

References

[1] Abbas, S. T., Mohammed, H. J., Ahmed, J. S., Rashid, A. S., Alhayani, B., & Alkhayyat, A. (2021). The optimization efficient energy cooperative communication image transmission over WSN. *Applied Nanoscience*, 1-13. https://doi.org/10.1007/s13204-021-02100-2

[2] Ávila, K., Sanmartin, P., Jabba, D., & Gómez, J. (2022). An analytical survey of attack scenario parameters on the techniques of attack mitigation in WSN. *Wireless Personal Communications*, *122*, 3687–3718. https://doi.org/10.1007/s11277-021-09107-6

[3] Daanoune, I., Abdennaceur, B., & Ballouk, A. (2021). A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks. *Ad Hoc Networks*, *114*, 102409. https://doi.org/10.1016/j.adhoc.2020.102409

[4] Elfarra, B. K., Salha, M. A., Rasheed, R. S., Aldahdooh, J., & Abusamra, A. A. (2023). Enhancing the Lifetime of WSN Using a Modified Ant Colony Optimization Algorithm. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *14*(3), 143-155. https://doi.org/10.58346/JOWUA.2023.I3.011

[5] Gao, K., Peng, R., Qu, L., Xing, L., Wang, S., & Wu, D. (2022). Linear system design with application in wireless sensor networks. *Journal of Industrial Information Integration*, *27*, 100279. https://doi.org/10.1016/j.jii.2021.100279

[6] Hema Kumar, M., Mohanraj, V., Suresh, Y., Senthilkumar, J., & Nagalalli, G. (2021). Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. *Journal of Ambient Intelligence and Humanized Computing*, *12*, 5287-5295. https://doi.org/10.1007/s12652-020-02007-w

[7] Jawad, G. A. M., Al-Qurabat, A. K. M., & Idrees, A. K. (2022). Maximizing the underwater wireless sensor networks' lifespan using BTC and MNP5 compression techniques. *Annals of Telecommunications*, *77*(9), 703-723. https://doi.org/10.1007/s12243-021-00903-6

[8] Keerthika, M., & Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. *Global Transitions Proceedings*, *2*(2), 362-367. https://doi.org/10.1016/j.gltp.2021.08.045

[9] Liang, J., Xu, Z., Xu, Y., Zhou, W., & Li, C. (2021). Adaptive cooperative routing transmission for energy heterogeneous wireless sensor networks. *Physical Communication*, *49*, 101460. https://doi.org/10.1016/j.phycom.2021.101460

[10] Moussa, N., Nurellari, E., & El Belrhiti El Alaoui, A. (2023). A novel energy-efficient and reliable ACO-based routing protocol for WSN-enabled forest fires detection. *Journal of Ambient Intelligence and Humanized Computing*, *14*(9), 11639-11655. https://doi.org/10.1007/s12652-022-03727-x

[11] Nabavi, S. R., Eraghi, N. O., & Torkestani, J. A. (2021). WSN routing protocol using a multiobjective greedy approach. *Wireless Communications and Mobile Computing*, *2021*(1), 6664669. https://doi.org/10.1155/2021/6664669

[12] Naeem, A., Javed, A. R., Rizwan, M., Abbas, S., Lin, J. C. W., & Gadekallu, T. R. (2021). DARE-SEP: A hybrid approach of distance aware residual energy-efficient SEP for WSN. *IEEE transactions on green communications and networking*, *5*(2), 611-621. https://doi.org/10.1109/TGCN.2021.3067885

[13] Patel, N. R., Kumar, S., & Singh, S. K. (2021). Energy and collision aware WSN routing protocol for sustainable and intelligent IoT applications. *IEEE Sensors Journal*, *21*(22), 25282-25292

[14] Prakash, M., & Prakash, A. (2023). Cluster Head Selection and Secured Routing Using Glowworm Swarm Algorithm and Hybrid Security Algorithm for Over IoT-WSNs. *International Academic Journal of Innovative Research*, *10*(2), 01–09. https://doi.org/10.9756/IAJIR/V10I2/IAJIR1004

[15] Ramya, R., & Brindha, T. (2022). A comprehensive review on optimal cluster head selection in WSN-IOT. *Advances in Engineering Software*, *171*, 103170. https://doi.org/10.1016/j.advengsoft.2022.103170

[16] Rezaeipanah, A., Amiri, P., Nazari, H., Mojarad, M., & Parvin, H. (2021). An energy-aware hybrid approach for wireless sensor networks using re-clustering-based multi-hop routing. *Wireless Personal Communications*, *120*(4), 3293-3314. https://doi.org/10.1007/s11277-021-08614-w

[17] Singh, O., Rishiwal, V., Chaudhry, R., & Yadav, M. (2021). Multi-objective optimization in WSN: Opportunities and challenges. *Wireless Personal Communications*, *121*(1), 127-152. https://doi.org/10.1007/s11277-021-08627-5

[18] Singh, S., & Saini, H. S. (2022). Intelligent ad-hoc-on demand multipath distance vector for wormhole attack in clustered WSN. *Wireless Personal Communications*, *122*(2), 1305-1327. https://doi.org/10.1007/s11277-021-08950-x

[19] Sreevidya, B., & Supriya, M. (2024). Malicious Nodes Detection and Avoidance Using Trust-based Routing in Critical Data Handling Wireless Sensor Network Applications. *Journal of Internet Services and Information Security*, *14*(3), 226-244. https://doi.org/10.58346/JISIS.2024.I3.013

[20] Suvarna, N. A., & Bharadwaj, D. (2024). Optimization of System Performance through Ant Colony Optimization: A Novel Task Scheduling and Information Management Strategy for Time-Critical Applications. *Indian Journal of Information Sources and Services*, *14*(2), 167-177. https://doi.org/10.51983/ijiss-2024.14.2.24

Authors Biography

G. Aravindh, pursuing his PhD degree in the area of wireless sensor networks. He obtained his M.E Degree in VLSI Design in 2015. Currently, he works as an Assistant Professor in the Department of Electronics and Communication (ECE) at P.A College of Engineering and Technology, Pollachi, Coimbatore. His research interests include Embedded Systems, Wireless Sensor Networks, and VLSI Signal Processing. He published 10 articles in the IEEE conference.

Capt. Dr.K.P. Sridhar, Professor & Head, Centre for Interdisciplinary Research, Karpagam Academy of Higher Education Coimbatore, Tamil Nadu, India. He obtained his Ph.D. degree in Robotics from Karpagam Academy of Higher Education. His research interests include Robotics, Artificial Intelligence, IoT, and Deep learning. He received research grants of More than 2 Crore from the Department of Science and Technology, New Delhi, India. He published 42 patents and has 52 granted patents. He published more than 35+ SCI, SCIE, and Scopus Indexed articles. He is the reviewer of IEEE Access, Wiley Black, and Springer Journals. He is the Prime Minister Awardee for start-up grants.