SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I8P104

Volume 11 Issue 8, 31-41, August 2024

Original Article

Improved Secure Distributed Routing Using Extended DART with Fault Avoidance and Queue-Based Load Balancing Protocol for WSN

B.R. Sathishkumar[1], B. Subbarayudu[2], P.M. Benson Mansingh[3], A. Senthilkumar[4]

[1]*Department of ECE, Sri Ramakrishna Engineering College, Tamilnadu, India.*
[2]*Department of ECE, Madanapalli Institute of Technology and Science, Andhra Pradesh, India.*
[3]*Department of Advanced Computer Science and Engineering, VIGNAN's Foundation for Science Technology and Research, Andhra Pradesh, India.*
[4]*Department of Computer Science with Data Analytics, Sri Ramakrishna College of Arts and Science, Tamilnadu, India.*

[1]*Corresponding Author : sathishkumar.b@srec.ac.in*

Received: 28 May 2024 Revised: 11 July 2024 Accepted: 05 August 2024 Published: 31 August 2024

Abstract *- Wireless Sensor Networks (WSNs), especially deployed wearing urbanized uses as automobile traffic surveillance, are the primary supply of serious details and create an enormous volume of information. Multipath routing kindness dependable details shipping and delivery within the situation of vulnerable information. Nevertheless, the drawback is the fact that lots of routes may boost the variety of command packets. This paper presents an advanced approach to secure distributed routing in WSNs, integrating Extended DART Fault Avoidance and Queue-based Load Balancing (DFAQLB). The proposed system aims to enhance the reliability and efficiency of routing mechanisms in challenging environments characterized by node failures and network congestion. The Extended DFAQLB offers robust fault tolerance capabilities by dynamically adjusting routing paths to circumvent faulty nodes and ensure reliable data delivery. Concurrently, the DFAQLB protocol optimizes network performance by distributing the traffic load across sensor nodes based on real-time queue monitoring and balancing strategies. Through extensive simulations and analysis, our results demonstrate significant improvements in network reliability, fault tolerance, and load distribution efficiency compared to traditional routing protocols. The proposed framework for enhancing the resilience and performance of WSNs deployed in mission-critical applications requires secure and efficient data transmission.*

Keywords *- Secure distributed routing, Wireless sensor network, Extended DART, Fault avoidance queue-based load balancing, Fault tolerance, Network reliability, Load distribution, Data transmission, Resilience.*

1. Introduction

The remarkable advancement in natural perspective technology enabled the development of microelectronics, leading to the production of tiny circuits and gadgets. Due to the installation and improvement of inexpensive equipment, correspondence engineering is undergoing a revolution that has sped up the design and development of WSNs at low cost and low power consumption [1].WSN has numerous uses to come down with the army and well-being of various manufacturing sectors. Routing is a technique used to find a path between a supply and a destination when information transfer is required. In WSN, information routing is performed at the system level. The routing table configuration provides a solution for this issue. It contains the node chance prospect lists for every given packet's location [2].

Numerous security concerns can arise from any routing technique, with Cluster Head (CH) attacks being among the most harmful. Due to source limitations, consumer's major used algorithms as Rivest Shamir Adelman (RSA), are challenging and energy-consuming for WSN. In several instances, several realizing component nodes are required to defeat green hurdles such as lines and obstructions of sight restrictions [3]. Furthermore, the environment being administered does not come with a connected level of current infrastructure for affordable electricity reception. Thus, it is important for realizing component nodes to make it through on small, limited energy sources of electrical power and talk by way of wireless reception. Protection might be an important problem due to natural limits in WSN [4].

Compared to existing ad hoc networks, WSNs have limited resources for learning, are heavily deployed, and are prone to issues. Additionally, WSNs have a much larger number of nodes than ad hoc networks, constantly changing network topologies, and typically use transmitted

correspondence platforms. Lastly, wireless sensor nodes in WSNs lack global identifying tags. Figure 1 illustrates the essential components of a typical WSN [5].

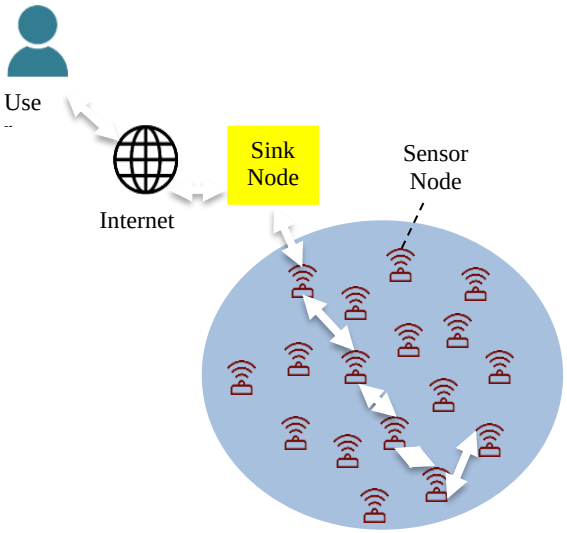


Fig. 1 Wireless sensor network architecture

This customization can enhance the performance and configuration of WSN. The topology and management of the network are also flexible and can be adjusted as per the requirements of specific applications. Mica motes, for instance, are designed to be stacked in tiers [6]. The central part of a mote is a low-power, low-resource computer that monitors one or more sensors, connects to the outside world via a wireless link, and communicates with other motes in the network. More often than not, they continued to be inside a standby method for energy-conserving objectives [7].

Likewise, the receptors generally capture their readings only one time each couple of minutes. Information is transmitted just once the mind is complete. Motes OS (MOS) forces mote applications to turn off except when particular situations that justify activity happen. The OS is additionally extremely modular. In case an application needs just particular features from MOS, the nonessential areas of the OS are instantly taken off the mote [8].

A WSN is typically deployed over a large area to collect data from its sensor nodes. These networks have numerous applications that are limited only by human imagination. This work provides an overview of various WSN attacks, primarily focusing on Denial of Service (DoS) attacks. It also summarizes the counterattacks available and provides a list of potential defenses. However, it should be noted that this document does not cover all preventative methods, nor does it provide a detailed analysis of every attack [9].

WSNs are one of the most well-known and promising technologies with various applications in medicine, industry, agriculture, household appliances, and the military. Scientists are working hard to make this technology ideal for different areas.WSN is defined as a network of nodes or devices that are tiny and have limited power and processing capability. These nodes collect multidimensional data and environmental sensing such as temperature and air pressure [10]. However, wireless communication raises serious security concerns because of numerous types of assaults like DoS attacks, node cloning, node capture, physical tampering, and others that may target it. Implementing a secure network is one of the core research difficulties, particularly because WSN is rapidly gaining impact in business, academia, and the military. This is because these nodes are physically constrained in size and resources [11].

WSNs are commonly used for monitoring combat zones, where security is of utmost importance. To ensure network integrity, secrecy, authentication, freshness, and scalability, it is essential to address these issues. Neglecting them can lead to serious security breaches, which can question the accuracy of the data. One of the most significant advantages of WSN is its ability to self-organize, enabling all nodes to work together seamlessly. However, removing security constraints for WSNs was a significant challenge for researchers. Traditional encryption and security techniques were not suitable for implementing WSN security due to constraints on available resources. Therefore, new approaches had to be developed specifically for WSN security [12].

WSNs consist of self-organizing sensor nodes that collect and analyze data about monitored objects in an area before sending it to the receiver. The first WSN emerged in the mid-20th century, combining wireless transmitters and sensors to collect data in real-time. Advancements in technology and research have contributed to the development of WSN, which is now used in various fields such as environmental monitoring, medical treatment, agricultural production, and preservation of cultural artifacts [13].

One of the most essential techniques used to protect information security is information encryption. Encryption converts plaintext into ciphertext, which is incomprehensible to others, using an encryption key and algorithm. Decryption is the process of converting ciphertext back into plaintext using an encryption key and algorithm. Encrypted text can only be decrypted by the person holding the decryption key [14].

There are two types of cryptosystems: symmetric cryptosystems and public key cryptosystems. In addition to common attacks like denial-of-service and eavesdropping, WSNs are vulnerable to node capture, counterfeiting, data tampering, and eavesdropping due to their deployment in unattended environments. Unfortunately, the current solutions for WSN security are subpar. As a result, users may find it difficult to adopt and install a WSN with adequate security and data protection. Until these security issues are resolved, the practical use of WSNs will remain limited [15].

1.1. Problem Statement

WSNs are utilized in diverse applications, ranging from industrial automation to environmental monitoring. However, these networks face challenges such as node failures, network congestion, and security vulnerabilities. Traditional routing protocols often struggle to cope with these challenges efficiently, leading to compromised network performance and reliability.

The problem addressed in this study is the need for an enhanced routing mechanism in WSNs that can ensure secure and reliable data transmission while effectively managing network resources. Specifically, the focus lies on mitigating the impact of node failures and alleviating congestion through efficient load-balancing strategies.

1.2. Research Gap

Existing fault avoidance and load balancing techniques in WSNs do not fully address the dynamic nature of these networks, where node conditions and network traffic patterns can change rapidly. Many traditional protocols cannot adapt to these changes in real-time, leading to network inefficiencies and increased vulnerability to failures and attacks.

There is a demand for a comprehensive solution that combines fault avoidance mechanisms with dynamic load balancing protocols to ensure uninterrupted data delivery and robust security in WSNs. Addressing these challenges is crucial for enabling WSNs to operate effectively in diverse environments, including those with limited resources and harsh conditions, while meeting stringent reliability and security requirements.

Existing research often focuses on either fault avoidance or load balancing independently without adequately addressing the interplay between these factors in dynamic WSN environments. The proposed DFAQLB protocol addresses these gaps by offering a holistic solution that combines dynamic fault avoidance, efficient load balancing, and integrated security, thereby advancing state-of-the-art WSN routing protocols.

2. Related Works

One of the main goals of setting up a WSN is to exchange information while ensuring the program's sustainability and preventing degradation through the use of strong resource management strategies [16]. The following list of investigation components influences how guiding events are constructed:

Node Setup: In a deep WSN, the node group varies depending on the application and may be manually selected or randomly assigned. When information is given manually, the receptors are precisely placed, and data is transmitted using predetermined techniques. Conversely, in an arbitrary design, the nodes are distributed randomly, resulting in a loosely appointed framework [17].

Use of Electricity: Battery longevity has a significant impact on sensor node lifespan. In a multi-bounce WSN, every node serves as both an information transmitter and an information switch. A few sensor nodes breaking down due to pressure frustration might cause significant topological changes, requiring rerouting of packages and method redesign [18].

Each sensor node within a WSN has a unique perspective of the surrounding world. However, each sensor's view is limited in terms of accuracy and breadth. It can only manage a small physical selection within the world. When transmitting data between nodes in a WSN, information exchange is essential. However, many sensor method applications require proficiency with node positioning. It can help reduce the impact of detrimental failure, which encourages early optimism for the miracle along the lines [19].

Routing protocols can be categorized into three types: Proactive, Hybrid, and Reactive. Proactive routing involves identifying the interactions that the system uses to transfer information from a source to a sink. With proactive routing, all possible routes are calculated beforehand, even before the sink starts communicating with the nodes of the system. On the other hand, reactive routing protocols only compute trail values when necessary [20].

Anytime a sink must get in touch with a certain node, the road values have been estimated, and amp; consequently, the very best course is selected for information transmission. Hybrid methods, as the title indicates, are a mix of equally reactive and proactive routing protocols, that make a decision when you should compute the route via the sink on the resource concerning the communication type [21].

It has been proposed that stationary nodes are better suited for hands-on routing techniques. The explanation is usually that much of the power may be protected when compared with reactive routing protocols that rely on finding the most effective course road for information transmission. For hands-on routing, it is not needed to look for the closest friends and neighbors for every subsequent hop when information is transmitted [22].

In a hierarchical architecture, nodes in a WSN perform various tasks and are often organized into groups based on their size or requirements. In hierarchical events, nodes are directly organized into organizations, and a node is selected as the CH, which is responsible for conglomerating information sent by the group using a conventional data fusion tool. The totaled information will be transmitted to the starting station in this fashion, decreasing vigor utilization. Literary works often contain various progressive concepts [23].

The LEACH process was the first and fundamental approach used for WSN which relied on class-dependent clustering. Position-based events utilize the location information of nodes to transmit necessary information to the designated location. Electricity advancements can be beneficial in location-based marketing events as they require information about the place to engage with nearby friends and neighbors effectively. This approach can help to reduce administrative expenses. Moreover, significant field information has to determine the splitting up between 2 particular nodes such that vigor utilization could be examined [24].

Cooperation-created routing protocols make use of high-level descriptors to get rid of unwanted details transmissions. Flooding is utilized to disseminate information, as a result of the point that flooding information is overlapped. Collisions can occur during transmissions, causing nodes to receive identical copies of information. As a result, the same content is repeatedly transported or altered between the same group of nodes, requiring a significant amount of power during this process.

Negotiation protocols such as SPIN are accustomed to controlling identical information and stopping unwanted details via being delivered to the subsequent neighboring node or perhaps towards the starting station by executing several negotiation communications within the true information that needs to be transmitted [25].

Multipath-blowing events have a go in the principle that increased delivery could be achieved by capturing much more than just one plausible manner. During the stage when many classes are acknowledged, whatever the reality which the vital means fizzles information giving might move forward constantly on another the majority of accessible methods without seated scarce for one more program being discovered. These protocols are effective in dealing with several paths. Nodes deliver the gathered information on several paths instead of making use of one track [26].

In this type of routing method, the system needs to consider both energy and quality. Whenever a sink in the system requests information from the sensing nodes, the transmission must meet specific QoS criteria, such as limited latency and bandwidth usage. Successive Assignment Routing (SAR) is one of the first routing solutions that incorporates the concept of QoS. SAR is based on three factors: energy consumption by the hubs and the sink, QoS of each element in the system, and the priority level of each cluster [27].

It is recommended that a good AODV guiding tradition be used for the ad hoc process. AODV includes 3 phases for being certain: program disclosure, program fix, and program assistance. During the program's disclosure phase, the end-to-end communication between the source of energy and the sink is established by flooding the course with requests for packages.

This particular treatment leads to a noteworthy increment of vigor utilization that constrains the selection of its remote sensor program. The author suggests an archival diet for statements. These archives store the authentications issued by the nodes themselves, along with a selected group of statements provided by others. However, the issue is that having an excess of statements in a sensor node could surpass its capabilities [28].

The Geographic and Energy Aware Routing (GEAR) protocol is introduced. It employs residual energy and geographical information of nodes to select the neighbors and guide the packets towards their destination. However, this technique has a higher cluster overhead and is not practical in a smart scenario. Another form of geographic routing called Geo-casting is also proposed. It combines multicast with geographical routing and transmits packets to nodes in a specific geographic area [29].

The most effective connection quality determines the matching metric. Minimizing retransmissions reduces power consumption. It has provided a looking forward to type of 2 traditions, for being certain, the supportive and quick traditions recalling the last goal to create a secured pair canny correspondence channel in between every 2 receptors. Ensuring the viability of the tradition and adaptability of the coalition of receptors is the key business program.

This demonstrates how the receptors are arranged with their corresponding keys. An important method to reveal the mysteries of a certain group of receptors involves a protective and flexible channel-based technique. This method encourages a specific set of receptors to conform to a standard feature, allowing for the establishment of a secure channel. To achieve this, a pseudo-random generation of unique codes is used for each secret group. The sensor IDs are used as seeds, and elements of relevance and importance are also taken into consideration during the process [30].

2.1. Research Gap

Although significant advancements have been made in load balancing and security in WSNs, there is a research gap in their integration into a unified framework. Specifically, existing literature tends to address load balancing and security as separate concerns rather than considering them holistically. This research gap presents an opportunity to develop a comprehensive approach that simultaneously addresses both load balancing and security challenges in WSNs. Some specific aspects of this research gap include:

Integration of Load Balancing and Security Mechanisms: Current research primarily focuses on either load-balancing techniques or security mechanisms independently. There is a lack of comprehensive frameworks that seamlessly integrate

load-balancing algorithms with robust security protocols tailored for WSNs. Adaptive Load Balancing with Security Considerations: While adaptive load balancing algorithms dynamically adjust to changing network conditions, they often overlook security considerations. Integrating adaptive load balancing with security mechanisms presents a research challenge in ensuring that dynamic load redistribution does not compromise.

Scalable and Efficient Solutions: Many existing load balancing and security approaches may lack scalability or efficiency when applied to large-scale WSNs with thousands of sensor nodes. Bridging this research gap requires the development of scalable and efficient solutions that can accommodate the unique characteristics and constraints of WSNs, such as limited computational resources, communication overhead, and energy consumption.

Evaluation and Validation in Real-world Scenarios: While theoretical proposals abound in the literature, there is a scarcity of empirical studies evaluating the practical effectiveness and feasibility of integrated load balancing and security solutions in real-world WSN deployments. Addressing this research gap necessitates conducting comprehensive empirical evaluations and validation experiments in diverse WSN environments to assess the performance, reliability, and security of proposed frameworks under realistic conditions.

Standardization and Adoption: The lack of standardized frameworks and protocols for integrated load balancing and security in WSNs hinders widespread adoption and deployment. Bridging this research gap involves collaborating with industry stakeholders, standardization bodies, and regulatory agencies to develop consensus-based standards and guidelines for secure and efficient WSN operation.

Closing this research gap requires interdisciplinary collaboration among researchers from fields such as computer science, telecommunications, cryptography, and control systems engineering. By addressing the integration of load balancing and security in WSNs, researchers can contribute to the development of more resilient, scalable, and secure WSN architectures capable of meeting the evolving demands of diverse applications.

3. Proposed System

A pioneering approach tailored to address the intricate challenges inherent in WSN. This protocol amalgamates several pivotal features to bolster the reliability, fault tolerance, and overall performance of WSNs.

Firstly, by leveraging secure distributed routing mechanisms, DFAQ-LB ensures the confidentiality, integrity, and authenticity of data traversing the network, fortified by cryptographic techniques and robust authentication mechanisms. Secondly, integrating Extended DART Fault Avoidance (EDFA) techniques builds upon the foundation of the Distributed Adaptive Routing Technique (DART), allowing DFAQ-LB to dynamically adapt routing paths to circumvent faulty nodes, thereby fortifying fault tolerance and enabling seamless data transmission, even amidst node failures or disruptions.

Thirdly, the protocol adopts a queue-based load-balancing strategy, meticulously monitoring queue lengths across nodes and dynamically redistributing data traffic to alleviate congestion and optimize resource utilization. This approach guarantees that the network workload is uniformly distributed, enhancing overall efficiency and performance. Additionally, DFAQ-LB is engineered to be adaptable to diverse network topologies, sizes, and environmental conditions, ensuring scalability and resilience in dynamic WSN environments.

Setting up the secrets together with the management note will conquer the secret secrets stealing procedure. Within the key discussing method, the dispersed information is estimated utilizing a k'1 amount polynomial. Several paths are utilized for simultaneous transmission, exactly where the initial information is split into n packets, and also, every package is transmitted around the many paths.

Figure 2 reveals the node communication of information making use of secret-sharing scheme-based dispersed information transfer. At this point, the initial information is dispersed directly into numerous packets in which the resource node transmits share packets on each road in which several shares are made with all the assistance of threshold quantity k. The threshold quantity plays the primary function while keeping the confidentiality of information transmission.

The authenticated information is decrypted soon after getting the k shares within the location node. The information revealed among the nodes utilizing several paths is carried out with a Galois area (GF). The bank account on the capture strikes is solved by executing the 8 packets. The multipath routing strategy tends to be more dependable and, additionally, probably the most secure strategy, but it has several disadvantages. The increased shares of the encrypted information enhance the probability of package damage. Furthermore, the cause node is liable for the number of variables for dispersed information and also the threshold quantity of the division of the information transfer.

3.1. Extended DART Fault Avoidance (ET-DFA)

To create several paths with a couple of joint nodes and bare minimum management packets, the ETDFA method has been built. The provided ETDFA is created for protected information transmission of WSN. The presented ETDFA includes two phases: routing table (Table 1) and DART (Topology and its routing tree Figure 3).

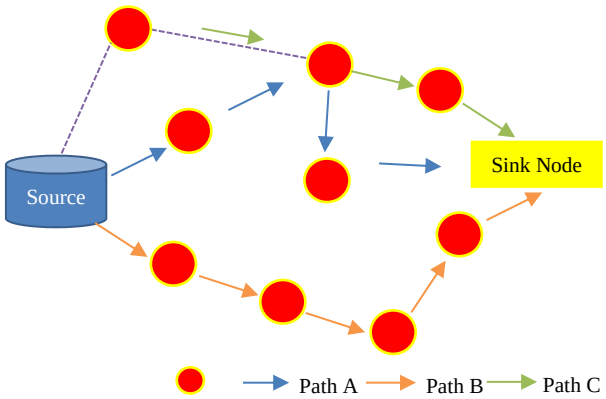
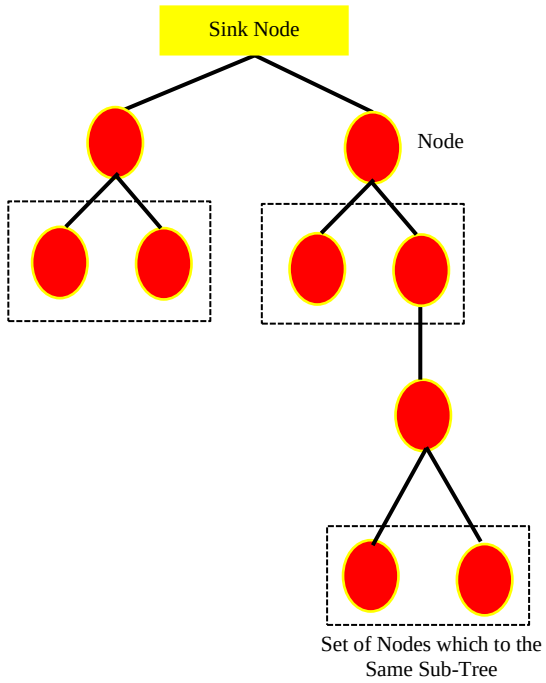
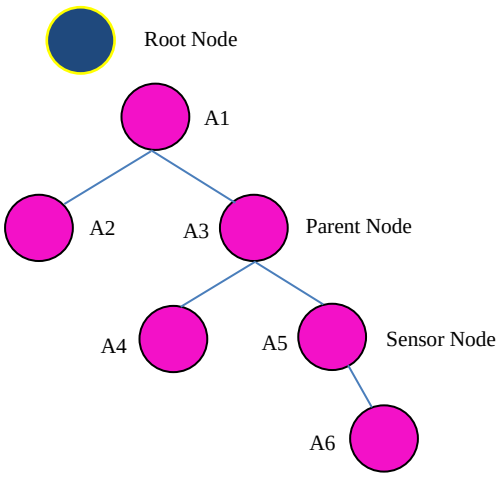


Fig. 2 Node communication



(a) Topology



b) Routing tree

Fig. 3 Topology and its routing tree

The use of the dining room table elimination method decreases the exchange of command packets within the networking and, therefore, brings down interference. The proposed work is made up of various characteristics, it could find many links disjoint several paths. It tries to browse many links and disjoint several paths; these paths are present. In the event it finds a set of website links disjoint numerous paths, it identifies a selection of contacts on the nodes within the paths. It creates a small quantity of management packets when producing many paths.

The secondary and primary capabilities count on history exploration results. The technique that's been proposed earlier must have 2 or even numerous disjoint paths to transmit information and secure decentralized details dispersion. Once the routing method explores many paths, it is proposed that the paths node disjoint. Nevertheless, checking out nodes disjoint several paths is composite and also may generate higher command packets. Within the method of protected decentralized details transmission, even though the joint node creates a weak point, the protected decentralized data transmission strategy may well stay away from the matter utilizing a good threshold quantity.

Table 1. Routing table

Designation	Next Hop
A1	A1
A2	A1
A3	A1
A4	A1
A5	A1
A6	A1
A2	A2
A3	A3
A4	A3
A5	A3
A6	A3
A4	A4
A5	A3
A6	A6

3.2. DART Fault Avoidance Queue-Based Load Balancing

Generally, community level comprising 3 subnets, there will be several routers attached within a few manners to facilitate unwanted backlinks for failover. These many backlinks are capable of being utilized for load balancing. Multipath routing will be the normal grouping for methods that include several routes to balance visitors throughout a selection of prospective paths. To deal with the issues earlier mentioned, a generic routing technique, DFAQ LB architecture is shown in Figure 4. Not restricted by a specific kind of community structure, that routing process could be utilized within every system architecture with normal topologies. FAQ-LB incorporates 3 parts, i.e., Fault Avoidance Queue mechanism to balance the product with routing table querying device.

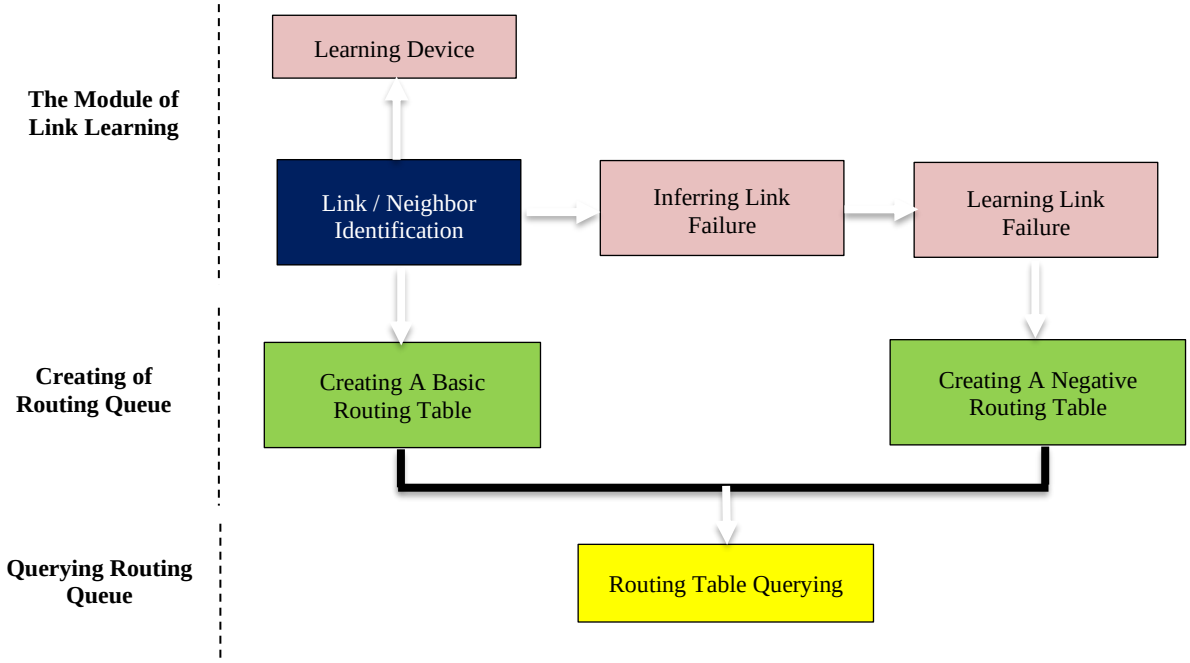


Fig. 4 Proposed DF AQ-LB model

Algorithm of DFAQ-LB

Step 1 : Receiver (D) received the data packet from Sender S through the shortest path
Step 2 : Analyse the outgoing and incoming data from every node
Step 3 : Reason analysis for dropping the original file into a trace file
Step 4 : If (drop == congestion || COL)
{
Step 4.1 : Assign the pktsize*qlim into qlimbytes
}
Step 5 : if (qlimbytes <= bytelength)
{
Step 5.1 : increment qlim
Step 5.2 : Assign the pktsize*qlim into qlimbytes
Step 5.3 : Increment the bytelength and assign it to q
}
Step 6 : If (Max-val<qlimitbyte)) //Overflow of queue
{
Step 6.1 : Compute outgoing and incoming data rate
}
Step 7 : if (available packet < rate)
{
Step 7.1 : Control the data rate by applying the TCP acknowledgment
}
Step 8 : From the sender side Sender (time, receiver_acknowledge, sequence_no)
{
Step 8.1 : Save all acknowledgement
Step 8.2 : Trace the file and time of capture of the acknowledgment saved
Step 8.3 : Save the sequence_no for acknowledgment
Step 8.4 : Compute the difference (delay) of acknowledgement
}
Step 9 : Compute the difference acknowledge2-acknowledge1 and save it into Old
Step 10 : Compare the delay
Step 11 : if (old<new)
{
Step 11.1 : Sender set the new rate
}
Else
{
Step 11.2 : Sender sends the actual rate
}

If the location is discovered, subsequently, the spot node transmits an acknowledgment to the sender node.DFAQ-LB appears upwards of the 2 routing queues to obtain the last appropriate paths.

4. Results and Discussion

The typical power usage of the command package with altering sink velocity for numerous protocols is illustrated in Figure 5. When the result is displayed within the graph, the management package overhead is extremely a lot less within the proposed method compared to the additional existing protocols. Within the railroad process, the rail building and station development is a one-time procedure.

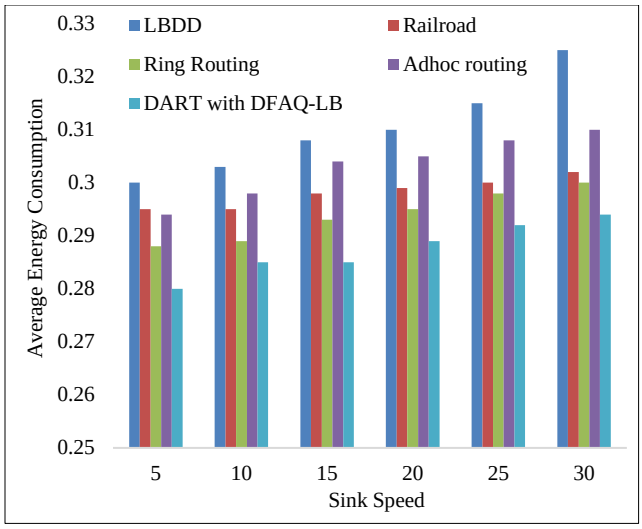


Fig. 5 Overhead control of packet

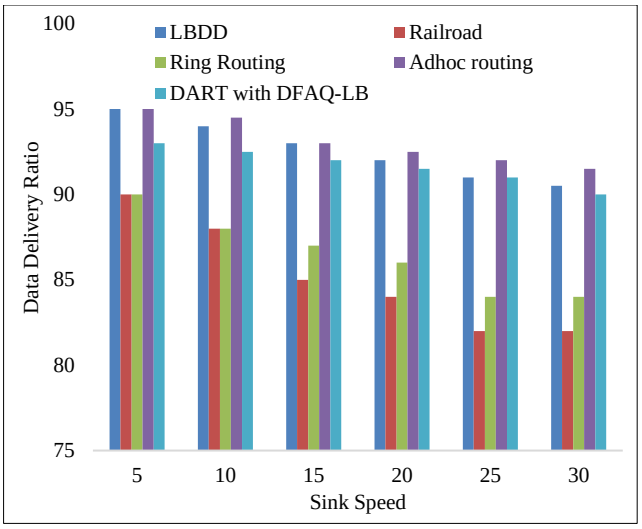


Fig. 8 Delivery ratio of packet

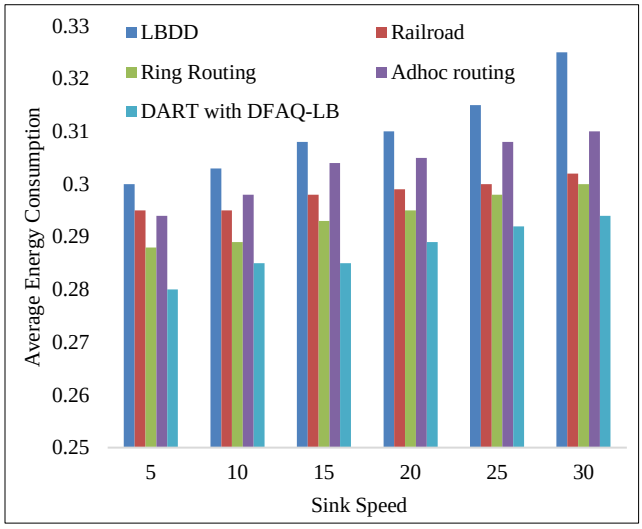


Fig. 6 Consumption of energy on average

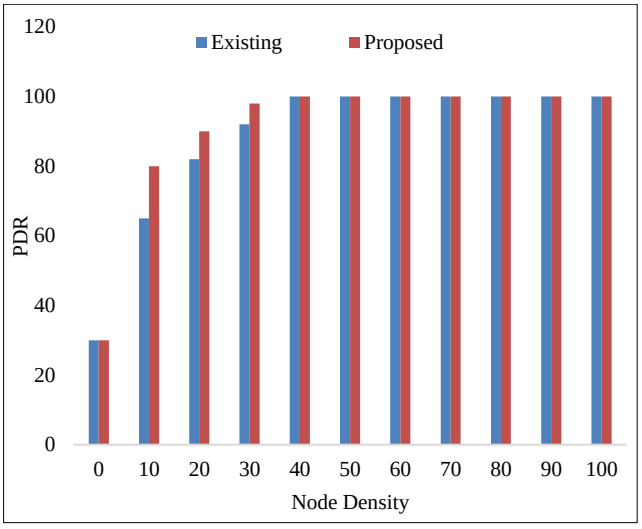


Fig. 9 Comparison of proposed methods with existing

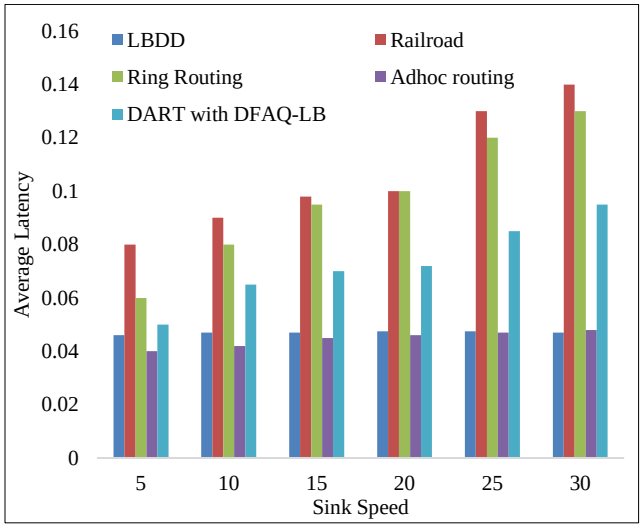


Fig. 7 Latency average

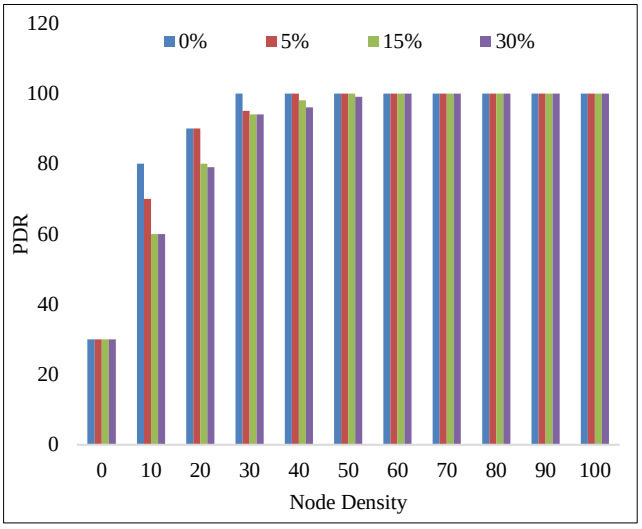


Fig. 10 Effect of routing circle occurrence in proposed DART with DFAQ-LB

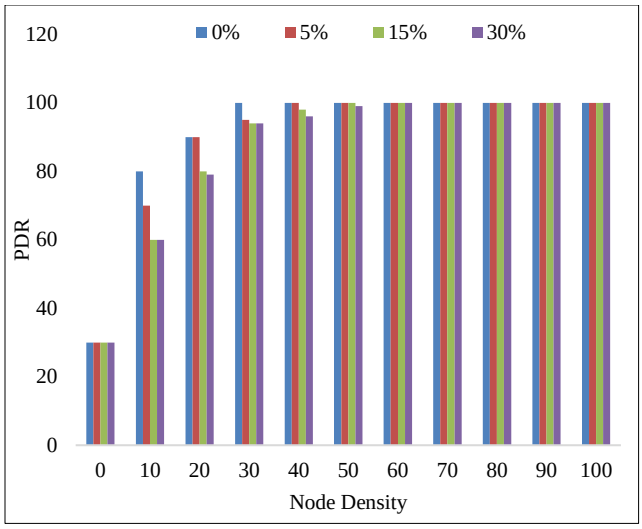


Fig. 11 Proposed DART with DFAQ-LB system to sinkhole attack

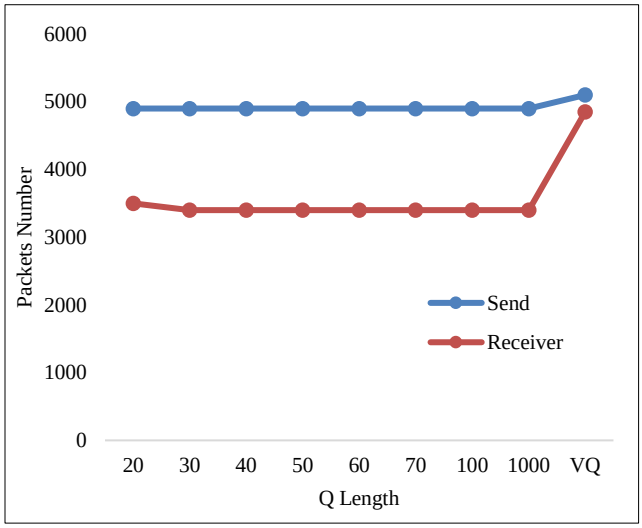


Fig. 12 Packet delivery ratio using DART with DFAQ-LB

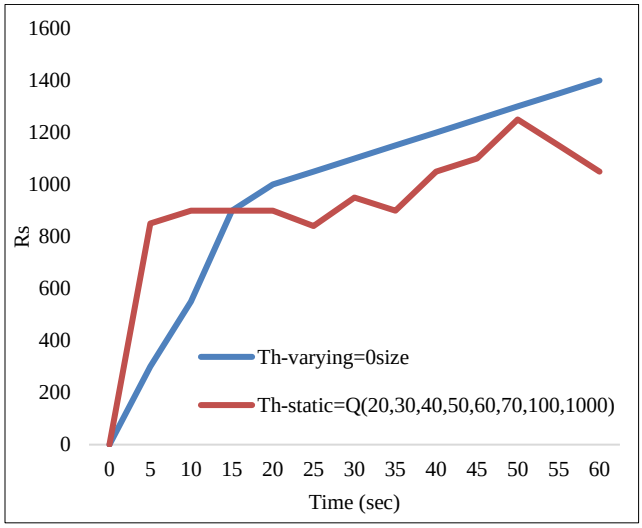


Fig. 13 Analysis of throughput using DART with DFAQ-LB

The entire power usage in every node for numerous protocols is displayed in Figure 6. The Proposed Method DART with DFAQ-LB does not need a sink area, though the common course measurements are bigger compared to Railroad, Ring routing, and Adhoc routing. Therefore the general power ingestion is much more and raises based on the sink velocity. The proposed method DART with DFAQ-LB requires a shorter time to supply the information as in comparison with Ring and Railroad routing. It is because of the smaller distance between the rendezvous area and the resource node is shown in Figure 7. The information transmission increases the delay. Within that particular period, the sink might relocate to a brand new spot that triggers information damage, as shown in Figure 8.

As illustrated in Figure 9, the proposed DART with DFAQ-LB is created to identify and stay away from the majority of the system-level strikes. Proposed strategy delivering phony info, changing transmitted packets, or maybe harming routing tables by outside assailants. Figure 10 presents the simulation outcomes for the effect routing loop strikes have on an unsecured community with various ratios of assailants, and the corresponding influence when proposed technique one is integrated into the routing process, correspondingly. Figure 11 displays the corresponding community PDR when the proposed DART with DFAQ-LBis is applied in the routing process. The DART with the DFAQ-LBmethod curve is extremely around the attack-free PDR curve, with about dropping fifteen % of automobiles as a result of their uncooperative behavior.

It is among the essential elements to determine the overall performance of the system. It estimated the foundation of the amount of packets obtained around the system by the amount of packets delivered, shown in Figures 12 and 13. The PDR functionality on the proposed DART with DFAQ-LB pattern is approximately ninety 5 % much more than the current SPIN and SPEED solutions. Hence the typical hold-off is extremely cut down comparatively.

5. Conclusion and Future Enhancement

A significant advancement in the domain of WSNs. Through the integration of secure distributed routing, DART with DFAQ-LB offers a holistic solution to the challenges of reliability, fault tolerance, and network efficiency in WSNs. The protocol's emphasis on secure distributed routing ensures the confidentiality, integrity, and authenticity of data transmission, safeguarding against security threats such as eavesdropping and tampering. By incorporating EDFA techniques, DART with DFAQ-LB enhances fault tolerance by dynamically adapting routing paths to bypass faulty nodes, thereby ensuring uninterrupted data delivery even in adverse network conditions. Moreover, the queue-based load balancing strategy employed by DART with DFAQ-LB optimizes resource utilization and alleviates network congestion by evenly distributing the workload across sensor

nodes. This approach enhances network efficiency and performance while mitigating the impact of traffic spikes and uneven data distribution.

Furthermore, DART with DFAQ-LB demonstrates adaptability and scalability, making it well-suited for deployment in diverse WSN environments with varying topologies and operational requirements. Through rigorous simulations and empirical validation, the protocol's effectiveness and feasibility have been thoroughly evaluated, showcasing its potential to advance the state-of-the-art in secure and efficient data routing in WSNs. In essence, DART with DFAQ-LB represents an improving solution to the multifaceted challenges faced by WSNs, offering a robust framework for enhancing reliability, fault tolerance, and network efficiency while ensuring the security and integrity of data transmission.

5.1. Future Enhancements

Dynamic Adaptation to Network Dynamics: Enhance FAQ-LB with adaptive mechanisms that can dynamically adjust routing paths and load balancing strategies based on real-time changes in network topology, traffic patterns, and environmental conditions. This would improve the protocol's resilience and responsiveness to dynamic network dynamics. Integration of Machine Learning Techniques: Incorporate machine learning algorithms to predict network traffic patterns, identify potential congestion points, and proactively adjust load balancing strategies accordingly. By leveraging historical data and real time analytics, FAQ-LB can optimize resource allocation and improve overall network performance.

Energy-Aware Routing and Load Balancing: Develop energy-efficient routing and load-balancing algorithms that prioritize the utilization of low-power nodes while ensuring balanced energy consumption across the network. This would extend the lifetime of battery-powered sensor nodes and enhance the sustainability of WSN deployments. QoS-aware Routing and Load Balancing: Introduce Quality of Service (QoS) metrics into FAQ-LB to prioritize critical data packets and ensure timely delivery of high-priority traffic. By considering factors such as packet loss, latency, and throughput, the protocol can better meet the diverse application requirements of WSNs.

Security Enhancement: Continuously enhance the security features of FAQ-LB to address emerging threats and vulnerabilities in WSNs. This may include integrating advanced encryption techniques, intrusion detection systems, and anomaly detection algorithms to detect and mitigate security breaches in real-time. Standardization and Interoperability: Work towards standardizing FAQ-LB protocols and interoperability frameworks to facilitate seamless integration with existing WSN infrastructures and interoperability with heterogeneous devices and networks. This would promote widespread adoption and compatibility across diverse WSN deployments.

Real-world Deployment and Validation: Conduct extensive field trials and real-world deployments of FAQ-LB in various application scenarios to validate its performance, scalability, and reliability in practical settings. This would provide valuable insights into the protocol's real-world feasibility and identify areas for further optimization and improvement. By pursuing these future enhancements, FAQ-LB can evolve into a more robust, adaptive, and efficient routing and load-balancing protocol for wireless sensor networks, addressing the evolving needs and challenges of emerging IoT applications.

References

[1] Abdelkader Benelhouri, Hafida Idrissi-Saba, and Jilali Antari, "An Evolutionary Routing Protocol for Load Balancing and QoS Enhancement in IoT-Enabled Heterogeneous WSNs," *Simulation Modelling Practice and Theory*, vol. 124, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] M. Revanesh, John M. Acken, and V. Sridhar, "DAG Block: Trust Aware Load Balanced Routing and Lightweight Authentication Encryption in WSN," *Future Generation Computer Systems*, vol. 140, pp. 402-421, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Nagesh Mallaiah Vaggu, and Ravi Sankar Barpanda, "DBlock-RLB: An Energy Efficient Framework for Intelligent Routing and Trading based Load Balancing in SDWSN Environment," *Ad Hoc Networks*, vol. 159, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] GSR Yogaraja, MN. Thippeswamy, and K. Venkatesh, "A Literature Study and Performance Gaps on Centralized Server-Based Load Balancing and Routing Strategies Under Cloud-IoT-WSN," *Australian Journal of Electrical and Electronics Engineering*, vol. 21, no. 2, pp. 138-160, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Majid Altuwairiqi, "An Optimized Multi-Hop Routing Protocol for Wireless Sensor Network Using Improved Honey Badger Optimization Algorithm for Efficient and Secure QoS," *Computer Communications*, vol. 214, pp. 244-259, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Najib Ahmed Mohammed, and Mohamed Othman, "A Load-Balanced Algorithm for Internet Gateway Placement in Backbone Wireless Mesh Networks," *Future Generation Computer Systems*, vol. 150, pp. 144-159, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] G. Ramani, and K. Amarendra, "An Optimized Energy Management and Load Balancing System Based on Cluster Head Selection for Vehicular Network Communication," *Multimedia Tools and Applications*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Huilong Jiang, "Exploration of Load Balancing Data Aggregation Algorithm in Wireless Sensor Network Based on Big Data Artificial Intelligence," *Internet Technology Letters*, vol. 7, no. 2, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Vishwas and K. Hareesh, "An Energy Efficient Cloud-Based Routing Protocol for Wireless Sensor Network (WSN) for Improving Throughput and Packet Delivery Ratio," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 13s, pp. 697-710, 2024. [Google Scholar] [Publisher Link]

[10] K. Dinesh, and SVN. Santhosh Kumar, "GWO-SMSLO: Grey Wolf Optimization-Based Clustering with Secured Modified Sea Lion Optimization Routing Algorithm in Wireless Sensor Networks," *Peer-to-Peer Networking and Applications*, vol. 17, pp. 585-611, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Neha Ahlawat, and Jasvinder Kaur, "A Mobility-Based Approach to Strengthen the Network Lifetime of Wireless Sensor Networks in 3D Region," *International Journal of Sensors Wireless Communications and Control*, vol. 14, no. 1, pp. 36-44, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mohammad Sirajuddin, and B. Sateesh Kumar, "Secure Power Aware Hybrid Routing Strategy for Large-Scale Wireless Sensor Networks," *International Journal of Computer Networks and Applications*, vol. 10, no. 6, pp. 1015-1029, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Harshvardhan Singh Chauhan et al., *Named Data Networking: Content Based Routing-Architecture Challenges and Applications* Emerging Technologies and the Application of WSN and IoT: Smart Surveillance, Public Security, and Safety Challenges, 1st ed., CRC Press, pp. 43-64, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jayantkumar A Rathod, and Manjunath Kotari, "TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol," *International Journal of Computer Networks and Applications*, vol. 11, no. 1, pp. 61-81, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Vishal Sharma, Rohit Beniwal, and Vinod Kumar, "Multi-Level Trust-Based Secure and Optimal IoT-WSN Routing for Environmental Monitoring Applications," *The Journal of Supercomputing*, vol. 80, pp. 11338-11381, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Liyazhou Hu et al., "Security Enhancement for Deep Reinforcement Learning-based Strategy in Energy-Efficient Wireless Sensor Networks," *Sensors*, vol. 24, no. 6, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] B.S. Venkatesh Prasad, and H.R. Roopashree, "Energy-Aware and Secure Routing for Hierarchical Cluster Through Trust Evaluation," *Measurement: Sensors*, vol. 33, pp. 1-8, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Anurag Shukla et al., "SEE2PK: Secure and Energy Efficient Protocol Based on Pairwise Key for Hierarchical Wireless Sensor Network," *Peer-to-Peer Networking and Applications*, vol. 17, pp. 701-721, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Shuaijie Li et al., "Analyzing the Robustness of LEO Satellite Networks Based on Two Different Attacks and Load Distribution Methods," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 34, no. 3, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Walid Osamy et al., "SEACDSC: Secure and Energy-Aware Clustering Based on Discrete Sand Cat Swarm Optimization for IoT-Enabled WSN Applications," *Wireless Networks*, vol. 30, pp. 2781-2800, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] S. Suresh Babu, and N. Geethanjali, "Lifetime Improvement of Wireless Sensor Networks by Employing Trust Index Optimized Cluster Head Routing (TIOCHR)," *Measurement: Sensors*, vol. 32, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Shiv Dutta Mishra, and Dipti Verma, "Energy-Efficient and Reliable Clustering with Optimized Scheduling and Routing for Wireless Sensor Networks," *Multimedia Tools and Applications*, vol. 83, pp. 68107–68133, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Hongzhang Han, Jun Tang, and Zhengjun Jing, "Wireless Sensor Network Routing Optimization Based on Improved Ant Colony Algorithm in the Internet of Things," *Heliyon*, vol. 10, no. 1, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Osama A. Khashan et al., "Innovative Energy-Efficient Proxy Re-Encryption for Secure Data Exchange in Wireless Sensor Networks," *IEEE Access*, vol.12, pp. 23290-23304, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Songhao Jia et al., "Research on WSN Intelligent Routing Algorithm Based on Bayesian Learning and Particle Swarm Optimization," *Recent Advances in Electrical & Electronic Engineering*, vol. 17, no. 3, pp. 304-315, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] Yogesh Patidar, Manish Jain, and Ajay Kumar Vyas, *Routing in Wireless Sensor Networks and Internet of Things: Systematic Analysis and Discussion*, AIoT and Smart Sensing Technologies for Smart Devices, Engineering Science Reference, pp. 181-196, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] M. Karthikeyan, D. Manimegalai, and Karthikeyan RajaGopal, "Firefly Algorithm-Based WSN-IoT Security Enhancement with Machine Learning for Intrusion Detection," *Scientific Reports*, vol. 14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] R. K. Krishna et al., "Hybrid Energy Balancer for Clustering and Routing Techniques to Enhance the Lifetime and Energy-Efficiency of Wireless Sensor Networks," *Journal of Autonomous Intelligence*, vol. 7, no. 2, pp. 1-10, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Tariq Mahmood et al., "Energy-Optimized Data Fusion Approach for Scalable Wireless Sensor Network Using Deep Learning-Based Scheme," *Journal of Network and Computer Applications*, vol. 224, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Amar Deep Gupta, and Ranjeet Kumar Rout, "SMEOR: Sink Mobility-Based Energy-Optimized Routing in Energy Harvesting-Enabled Wireless Sensor Network," *International Journal of Communication Systems*, vol. 37, no. 4, 2023. [CrossRef] [Google Scholar] [Publisher Link]