International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223695 Volume 10, Issue 6, November – December (2023)

RESEARCH ARTICLE

Secure Power Aware Hybrid Routing Strategy for Large-Scale Wireless Sensor Networks

Mohammad Sirajuddin
Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India.
mohdsiraj569@gmail.com

B. Sateesh Kumar
Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, University College of Engineering, Jagitial, Telangana, India.
sateeshbkumar@jntuh.ac.in

Received: 23 September 2023 / Revised: 30 November 2023 / Accepted: 11 December 2023 / Published: 30 December 2023

Abstract – Wireless Sensor Networks (WSNs) in critical applications demand safe routing methods to increase network life and protect data flow. This study proposes a "Secure Power Aware Hybrid Routing Strategy for Wireless Sensor Networks (WSN) utilizing randomized cluster head selection" to address these challenges. Traditional routing systems typically face energy depletion because of uneven node energy usage and attacks. The recommended strategy uses clustering and randomization to overcome these concerns. The network is divided into clusters with dynamically designated cluster heads. Randomly selecting cluster heads (CHs) in a network strengthens it against attacks targeting fixed CHs. Thus, this randomization method enhances network security. Energy efficiency is critical in Wireless Sensor Networks. This method solves the problem by considering power while choosing cluster heads. Assigning greater probability to nodes with more residual energy for cluster head (CH) selection encourages fairer energy utilization throughout the network, extending its operational lifetime. The research also evaluates the technique's energy usage, network longevity, and security robustness. The approach is tested against conventional routing techniques in simulated tests. The research found that the proposed technique outperforms existing methods in energy efficiency, network lifetime, and security. The hybrid technique combines clustering with randomization to provide a more adaptable and safe network architecture. Finally, the proposed technology may improve Wireless Sensor Network energy efficiency and security. The hybrid strategy balances energy savings and network protection. This makes it excellent for a broad variety of critical sector applications that prioritize reliability, longevity, and data integrity.

Index Terms – Secure, Power Aware, Hybrid Routing, Selective Routing, WSN, Randomized Cluster Head Selection.

1. INTRODUCTION

The expansion of Wireless Sensor Networks (WSNs) in recent years has led to notable breakthroughs in several sectors, including environmental monitoring, industrial automation, and healthcare applications. These networks are comprised of several tiny sensor nodes that have little power, but are endowed with capabilities for sensing, processing, and wireless communication. These nodes collaborate to gather and communicate data from the environment being monitored. Nevertheless, the intrinsic limitations of Wireless Sensor Networks (WSNs), including restricted energy resources, confined processing capabilities, and vulnerability to diverse security threats, provide complex obstacles to their efficient and continuous functioning [1].

One of the foremost considerations in Wireless Sensor Networks (WSNs) pertains to the optimal exploitation of energy resources. The impracticality of recharging energy in sensor nodes is generally attributed to the distant and harsh deployment circumstances they are often subjected to. Hence, the durability of the network is largely contingent upon the use of prudent energy management measures [2]. Traditional routing systems tend to unevenly distribute energy consumption across the network, resulting in some nodes experiencing a quick depletion of energy. This ultimately restricts the total lifetime of the network. The investigation of strategies for achieving equilibrium in energy use, with the aim of optimizing the duration of network functionality, continues to be a prominent area of scholarly inquiry.

Simultaneously, the security of Wireless Sensor Networks (WSNs) has significant significance, particularly due to their growing use in crucial domains such as military surveillance, environmental monitoring in disaster-prone regions, and healthcare systems. Wireless Sensor Networks (WSNs) are vulnerable to a wide range of assaults due to their inherent wireless communication capabilities. These attacks include eavesdropping, data manipulation, node compromise, and

RESEARCH ARTICLE

denial-of-service attacks [3]. Conventional routing protocols often lack the necessary capabilities to address security risks adequately. Consequently, it becomes imperative to devise resilient techniques that not only ensure the protection of data transfer but also successfully counter prospective assaults.

This research presents a novel technique, referred to as the "Secure Power Aware Hybrid Routing Strategy for Wireless Sensor Networks (WSNs) with randomized cluster head selection." The proposed strategy addresses the interconnected issues of energy efficiency and security in WSNs. The suggested technique aims to strike a compromise between energy saving and network resilience by integrating the advantages of clustering and randomization. The use of a randomized strategy in the strategic selection of cluster heads (CHs) contributes to the enhancement of the network's resilience against targeted assaults, as well as the facilitation of a balanced distribution of energy consumption [4]. In addition, the incorporation of nodes' residual energy levels during the process of selecting cluster heads (CHs) serves to prolong the overall operational lifespan of the network.

This research seeks to make a scholarly contribution to the field of Wireless Sensor Networks (WSNs) by proposing a new routing approach that combines power-awareness and security concerns. This technique has the potential to significantly transform the design and operation of Wireless Sensor Networks (WSNs) in critical applications. It aims to tackle the interconnected difficulties of energy efficiency and network protection, which are crucial for ensuring dependability, sustainability, and data integrity in such applications.

This article's subsequent segment is organized into distinct sections. Section 2 provides a comprehensive overview of the available routing methods. Section 3 addresses the problem statement, while Section 4 delineates the proposed criteria for Cluster Head determination and the Secure Selective Routing technique. Section 5 delves into the results and discussions, and Section 6 offers an in-depth comparative analysis. Finally, Section 7 concludes the article.

2. RELATED WORK

The field of Wireless Sensor Networks (WSNs) has seen a multitude of research endeavors focused on improving the security, energy efficiency, and overall performance of these networks. This literature study aims to examine a range of significant scholarly contributions, providing insights into the suggested systems, their respective advantages, and their inherent constraints.

The authors Ahutu and El-Ocla (2020) presented a research paper titled "Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks" [5]. The protocol developed by the researchers aim to effectively identify wormhole assaults by implementing a centralized control mechanism. This approach is designed to tackle the urgent challenge posed by such attacks. Although the network's capacity to detect is effective, its centralized form may expose it to vulnerabilities such as single points of failure and scalability challenges.

In a scholarly article, Alghamdi (2018) introduced a novel approach titled "Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method" [6]. This approach integrates route optimization with the utilization of Diffie-Hellman (DH) cryptography. Although DH cryptography enhances security, it may result in increased processing overhead, which might have implications for energy efficiency in nodes with limited resources.

In their study, Alotaibi (2021) presented a novel approach to secure routing in IoT-based wireless sensor networks (WSNs) by using an enhanced version of the Blowfish algorithm [7]. The used methodology utilizes the Blowfish algorithm to augment the level of security. Nevertheless, the use of cryptographic algorithms in IoT-based wireless sensor networks (WSNs) may result in the introduction of delay as a consequence of the processing overhead. This latency has the potential to impede the seamless operation of real-time applications inside such networks.

The study conducted by Bin-Yahya et al. (2022) centered on the topic of "Securing Software-Defined Wireless Sensor Networks Communication through the Implementation of Trust Management" [8]. The focal point of their methodology is on the enhancement of communication security by means of trust management. Nonetheless, the formation and administration of trust might result in an increase in resource use, posing difficulties in the implementation of trust mechanisms inside dynamic networks.

In a previous study, Bin-Yahya and Shen (2023) presented a research paper titled "Secure and Energy-Efficient Network Topology Obfuscation for Software-Defined Wireless Sensor Networks" [9]. The implemented approach improves security by deliberately obscuring the network's topology. However, the implementation of the obfuscation process may lead to potential communication delays as a consequence of heightened processing demands.

In addition to the aforementioned features, the realm of Wireless Sensor Network (WSN) study encompasses several more dimensions. Chatterjee and colleagues (2021) released a research paper titled "IPLQueeN: Integrity Preserving Low-Overhead Query Handling Over NDN-Based WSN" [10]. The paper focuses on the topic of query management while ensuring integrity preservation. Although this strategy is unique, it may potentially result in an increase in communication overhead during the treatment of queries. In their publication titled "Joint Energy-Saving Scheduling and

RESEARCH ARTICLE

Secure Routing for Critical Event Reporting in Wireless Sensor Networks" (Feng et al., 2020), the authors introduced a novel approach. The collaborative optimization technique used by the authors focuses on the issue of crucial event reporting, while simultaneously prioritizing energy saving [11]. However, the simultaneous attainment of energy savings and security may give rise to intricate trade-offs.

The study conducted by Fu et al. (2021) addressed the challenges posed by harsh settings via the development of a "Sustainable Multipath Routing Protocol for Multi-Sink Wireless Sensor Networks in Harsh Environments" [12]. This protocol places a strong emphasis on the concept of sustainability. However, the difficulties presented by inhospitable surroundings need ongoing adjustments, which may have an influence on the efficacy of the procedure.

In the domain of security, the study conducted by Gope et al. (2017) delved into the topic of resilience against Denial of Service (DoS) attacks. The authors specifically focused on the resilience of DoS attacks in the context of designing an anonymous user authentication protocol for wireless sensor networks, as outlined in their publication titled "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks" [13]. The research conducted by the authors highlights the significance of maintaining anonymity, however it may encounter obstacles in terms of scalability when used in networks of considerable size.

The authors Haseeb et al. (2020) presented a research paper titled "Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network" [14], which emphasizes the importance of energy efficiency and security considerations in the context of wireless sensor networks. The inherent conflict between optimizing energy efficiency and ensuring security is a persistent difficulty in the implementation of these protocols.

The study topic of Wireless Sensor Networks (WSNs) is characterized by an ongoing pursuit of routing protocols that prioritize security, energy efficiency, and reliability. This literature review offers a comprehensive analysis of several suggested systems, emphasizing their respective contributions, strengths, and limitations.

The paper titled "Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network" was presented by Haseeb et al. (2020) [15]. The protocol presented in their study aims to effectively tackle the issues of security and energy efficiency by using a heuristic method. Although the protocol exhibits potential in addressing the trade-off between security and energy considerations, the efficacy of heuristics may differ depending on the specific network conditions.

The authors Haseeb et al. (2019) introduced a framework for intrusion prevention in secure routing within the context of WSN-based Mobile Internet of Things (IoT) [16]. The framework's objective is to mitigate intrusions in Internet of Things (IoT)-based Wireless Sensor Networks (WSNs). Nevertheless, the efficacy of the framework may be contingent upon the breadth and complexity of possible incursions.

In a separate study, Haseeb et al. (2019) introduced a research paper titled "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for Internet of Things (IoT) Based Wireless Sensor Networks" [17]. The protocol proposed by the authors incorporates the concept of secret sharing in order to enhance energy efficiency. However, the introduction of secret sharing systems may have implications for scalability and resource use.

In their study, Hatzivasilis et al. (2017) made a significant contribution by introducing the concept of "SCOTRES: Secure Routing for IoT and CPS" [18]. This research focused on the development of secure routing protocols specifically designed for the Internet of Things (IoT) and Cyber-Physical Systems (CPS). The suggested method improves security; nevertheless, further research is needed to assess the feasibility and flexibility of using the system in various Internet of Things (IoT) and Cyber-Physical Systems (CPS) contexts.

In their publication, Li et al. (2014) introduced a routing protocol titled "Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks" [19]. The protocol places significant emphasis on load balancing inside service-oriented WSNs. However, the pursuit of load balancing while simultaneously upholding security measures may result in compromises between the distribution of data and the establishment of safe communication channels.

The paper titled "Active Trust: Secure and Trustable Routing in Wireless Sensor Networks" (Liu et al., 2016) highlights the significance of safe and trustworthy routing in wireless sensor networks [20]. While this particular strategy emphasizes the importance of ensuring security, it is worth noting that the additional burden of creating trust connections may have a detrimental effect on the scalability of the network.

The study conducted by Mutalemwa and Shin (2021) investigated the use of innovative strategies to enhance the reliability of location privacy protocols in the monitoring of wireless networks [21]. The research mostly focuses on methods pertaining to the preservation of location privacy. However, the attainment of both dependability and privacy may need intricate protocol designs.

In their study, Pathak et al. (2022) introduced a novel routing algorithm for Wireless Sensor Networks (WSNs) titled "Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs" [22]. The algorithm used utilizes

RESEARCH ARTICLE

Quality of Service (QoS) and trust mechanisms to boost both security and performance. However, the examination into the algorithm's capacity to adapt to constantly changing network circumstances continues.

The study conducted by Qin et al. (2017) made a significant contribution to the field of wireless sensor networks with their research on a secure routing mechanism that is based on trust sensing [23]. The authors' study presents a secure routing system that utilizes trust sensing. Nevertheless, the constant evaluation of trust sensing systems is necessary to accurately capture the dynamic nature of network trustworthiness.

The research landscape of Wireless Sensor Networks (WSNs) is abundant with creative concepts that seek to improve security, efficiency, and dependability across several facets of network operation. The present literature review examines number of research, highlighting their respective suggested systems, contributions, and inherent limitations.

The authors Rathee et al. (2021) proposed a routing algorithm for wireless sensor networks that focuses on energy balancing, quality of service, and security. The algorithm is based on ant colony optimization and aims to optimize the energy consumption of the network while ensuring reliable and secure data transmission [24]. The proposed approach integrates ant colony optimization and energy balancing techniques to provide Quality of Service (QoS)-aware secure routing. Nevertheless, the potential drawbacks linked to ant colony optimization might potentially hinder the real-time performance inside dynamic situations.

The study conducted by Roy et al. (2014) made a significant contribution to the field of wireless sensor networks by addressing the issue of secure data aggregation. Their research focused on mitigating the impact of attackers on the aggregation process, as discussed in their publication titled "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact" [25]. The research conducted by the authors focuses on the topic of safe data aggregation, specifically emphasizing the mitigation of attackers' influence via the use of filtering techniques. Although the suggested filtering algorithms are successful, they have the potential to contribute complexity to the network design.

The research conducted by Saleem et al. (2014) focused on the empirical examination of a bio-inspired self-organized secure autonomous routing protocol [26]. The protocol under consideration places emphasis on the establishment of secure routing by self-organization, using principles inspired by biological processes. However, the execution of these protocols may need substantial processing resources, hence affecting scalability.

The authors Salim et al. (2021) put up a research paper titled "A Secure Data Gathering Scheme Based on Properties of Primes and Compressive Sensing for Internet of Things (IoT)-Based Wireless Sensor Networks (WSNs)" [27]. The proposed methodology places significant emphasis on the safe acquisition of data by leveraging prime qualities and using compressive sensing techniques. Nevertheless, the dependence on prime qualities may potentially expose vulnerabilities to assaults that leverage the principles of number theory.

In their publication titled "Secure Source-Based Loose Synchronization (SOBAS) for Wireless Sensor Networks" (Uluagac et al., 2013), the authors presented a novel synchronization technique [28]. The suggested synchronization approach exhibits an improvement in security; nonetheless, it is essential to do more investigation into the potential ramifications of synchronization delays on network performance.

The study conducted by Verma et al. (2022) investigated the topic of "Intelligent and Secure Clustering in Wireless Sensor Network (WSN)-Based Intelligent Transportation Systems" [29]. The research conducted by the author centers on the topic of intelligent and safe clustering inside wireless sensor networks (WSNs) that are specifically designed for transportation applications. However, the actual use of intelligent clustering may require the utilization of computationally demanding methods and result in additional computational burden.

The author Alkanhel et al. (2023) innovatively integrated a Multi-swarm optimization procedure with a genetic algorithm to bolster the network's longevity. The mathematical representation of the fitness function facilitated improved data transmission [30]. Although this approach demonstrated remarkable efficiency, its potential complexity in implementation arises from the sophisticated optimization processes employed.

The author Misbha et al. (2023) introduced an innovative and energy-efficient lightweight key distribution mechanism. In the initial phase, the system strategically identifies the optimal cluster head for efficient clustering, employing criteria such as Signal Strength Indicator, energy levels, delay, and distance. Subsequently, the data transfer process ensues, with the proposed technique ensuring secure transmission [31]. This methodology employs session key generation as a protective measure to secure the encryption key during the entire process.

These papers together demonstrate the ever-evolving nature of research in Wireless Sensor Networks (WSNs). Each solution offered provides useful insights into addressing certain difficulties, but also has possible limitations in terms of scalability, complexity, and resource utilization. As wireless sensor networks (WSNs) undergo further advancements, their contributions play a significant role in the continuous progress

RESEARCH ARTICLE

towards the creation of efficient, secure, and dependable solutions.

These literature reviews present a comprehensive overview of the many methodologies used to improve routing protocols in Wireless Sensor Networks (WSNs). Each solution under consideration aims to tackle distinct difficulties; nevertheless, they also encounter restrictions pertaining to scalability, complexity, and trade-offs. The collective information produced by these works helps to advance resilient and flexible routing solutions in the ever-changing domain of Wireless Sensor Networks (WSNs).

The related works with higher impacts are summarized in Table 1.

Table 1 Summary of Related Works

Author, Year	Proposed Method	Limitations
Ahutu et al. [5], 2020	Centralized Routing Protocol	The centralized routing system that has been suggested may encounter difficulties in the context of large-scale wireless sensor networks, mostly owing to the amplified overhead and processing demands that are inherent to centralized management.
Alotaibi et al. [7], 2021	Blowfish	The practical usefulness of the modified Blowfish algorithm-based secure routing approach must be evaluated via testing and validation in real-world situations of IoT-based wireless sensor networks.
Bin-Yahya et al. [8], 2022	Trust Management	The incorporation and administration of trust mechanisms inside software-defined wireless sensor networks may result in increased intricacy and resource use, as well as potential delays in communication.
Bin-Yahya et al. [9], 2023	Topology Obfuscation	The implemented approach improves security by deliberately obscuring the network's topology. However, the implementation of the obfuscation process may lead to potential communication delays as a consequence of heightened processing demands.
Chatterjee et al. [10], 2021	Query Handling	It is essential to assess the performance and efficacy of the proposed IPLQueeN protocol over a range of network sizes, traffic loads, and attack scenarios in order to ascertain its suitability under different settings.
Fu et al. [12], 2021	Multipath Routing	Further testing may be required to evaluate the efficacy of the sustainable multipath routing protocol in challenging contexts, taking into consideration the potential influence of diverse environmental circumstances on its performance.
Haseeb et al. [15], 2020	Heuristic Routing	It is essential to thoroughly evaluate the trade-offs between security advances and energy consumption of the energy-aware heuristic routing protocol, with a particular emphasis on network lifespan preservation, in order to effectively address security concerns.
Pathak et al. [22], 2022	Adaptive QoS	The practical implementation constraints of the adaptive Quality of Service (QoS) and trust-based lightweight secure routing algorithm pertain to their compatibility with diverse hardware and software platforms, necessitating attention for successful deployment in real-world scenarios.
Verma et al. [29], 2022	Secure Clustering	The scalability and flexibility of the intelligent and secure clustering technique should be assessed in the context of bigger and more intricate intelligent transportation systems that rely on wireless sensor networks.
Alkanhel et al [30], 2023	Fitness Function	This method's practical application could pose challenges due to the intricate nature of the advanced optimization processes entailed. Its implementation may demand a nuanced understanding of the sophisticated optimization mechanisms involved, potentially complex during deployment.

RESEARCH ARTICLE

3. PROBLEM STATEMENT

The growing use of wireless sensor networks (WSNs), which make it easier to gather and transmit data across long distances, has ushered in substantial changes across a variety of business sectors. Despite this, a few challenges have made it difficult for these systems to achieve their full potential in terms of performance and lifespan. These challenges include, but are not limited to, a limited supply of energy, inequities in energy use, and susceptibility to security risks. The goal of the current research is to address the following difficulties.

The phenomena of energy imbalance and the effect that it has on the decreased lifetime of networks is a topic of study in the academic community.

In wireless sensor networks (WSNs), the use of standard routing strategies often leads to uneven energy consumption patterns. This is because certain nodes face rapid energy depletion, while others continue to be underused. The difference causes unexpected malfunctions in the network, which in turn shortens the total amount of time that operations may be carried out successfully.

Because Wireless Sensor Networks (WSNs) have intrinsic features such as open wireless communication and restricted resources, they are susceptible to security assaults. This makes them a target for cybercriminals. Traditional routing systems have limits in their ability to effectively combat attacks such as node compromise, data manipulation, and denial-of-service, which poses a danger to the network's resilience and the data's integrity. Traditional routing systems also have limitations in their capacity to properly route traffic.

The present routing algorithms, which employ predetermined selections for cluster heads (CH), have a limited ability to resist targeted attacks. These assaults make use of the predictable nature of CH placements in order to gain an edge. It is possible for adversaries to direct the majority of their efforts on penetrating these stationary communication hubs (CHs), which would then result in broad disruption of the network as well as the compromise of data.

When it comes to wireless sensor networks (WSNs), conserving energy is of the highest significance to extending the total lifespan of the network. When choosing cluster heads, the current routing algorithms do not adequately take into consideration the energy levels of the individual nodes, which results in an unbalanced distribution of energy and inefficient use of energy resources.

Planning or selecting one course of action over another (or more) possibilities is what we mean when we talk about making a trade-off. The dynamic relationship between effective use of energy and safety.

It is a difficult task to create Wireless Sensor Networks (WSNs) that successfully combine high levels of energy efficiency with stringent levels of data protection. Implementing innovative routing algorithms that are able to dynamically adapt to changing network conditions and possible dangers is necessary in order to achieve efficient energy usage while also maintaining stringent security measures. This is a requirement for achieving the goal of achieving efficient energy use while keeping robust security measures.

4. PROPOSED METHODOLOGY

In this section of the work, the two prime problem solutions are discussed.

4.1. Selecting Cluster Head

Firstly, the cluster head selection process is discussed. WSN (Wireless Sensor Network) cluster head selection is a pivotal process in optimizing network efficiency. This intricate task involves designating a few sensors as cluster heads to manage communication and data aggregation, reducing energy consumption, and enhancing the overall system lifespan. The selection process's effectiveness significantly impacts network performance and resource utilization.

Assuming that, the total network is represented as SN[ ] and each node in the network is identified as N_i. Thus, for n number of nodes, this is denoted by equation (1).

$$SN[\,] =< N_1, N_2, N_3, \ldots . N_n > \quad (1)$$

All the nodes in the network are identified distinctly with the collection of parameters such as battery level, $BT(t)_i$, connectivity between the other nodes, GN_i, as a sub-graph and the mobility factor M_i. Thus, combined it is resented by equation (2).

$$N_i = [BT_i(t), GN_i, M_i] \quad (2)$$

Whereas the total network connectivity, G[ ] can be presented by equation (3),

$$G[\,] = [G_1, G_2, \ldots . G_n] \quad (3)$$

Now for selecting the cluster head selectively and randomly to increase the network lifetime, few characteristics are to be ensured.

Initially, the potential cluster head, N_{CH}[ ] must be nearer to the source node, N_i. The nearest nodes can be identified from the network graph formulated by equation (4).

$$N_{CH}[\,] = N_i | G_i = N_i ::[N_j, \ldots . N_{(i+m)}] \quad (4)$$

For “m” number of neighboring nodes.

Further, the battery level in these selected nodes must be high and the neighboring node having the highest battery levels must be selected it is denoted by equation (5),

$$N'_{CH}[\,] = \prod_{BT=High} N_{CH}[i].BT(t) \quad (5)$$

RESEARCH ARTICLE

Regardless of the mention, the sub-selected nodes also must have good connectivity between the other nodes as well. Thus, the following selection ensures that it is shown in equation (6).

$$N''_{CH}[\,] = \prod_{G=High} N'_{CH}[\,].G[i] :: SN[\,] \quad (6)$$

Nonetheless, a selected cluster head must have a low mobility to ensure that the selected routing path is stable. Thus, the following selection as shown in equation (7), will ensure to select a cluster head as,

$$N_{CH}[\,] = \prod_{M=Low} N''_{CH}[\,].M(i) \quad (6)$$

Henceforth, using this method, the cluster head selection algorithm is designed and furnished.

Input:

- Every node inside the network has data pertaining to its battery status, mobility, and communication with other nodes.
- The three thresholds that are relevant to this discussion are the battery threshold (Bt), mobility threshold (Mt), and connection threshold (Ct).

Output:

- The cluster head(s) that have been chosen.

Assumption:

- Each sensor node is assigned a unique identifier.
- The battery level is quantified as a percentage ranging from 0 to 100%.
- The concept of mobility may be described as the measure of the speed at which a node moves during a certain timeframe.
- Connectivity is quantified by the quantity of neighboring nodes with whom a given node is capable of establishing communication.

Process:

Step -1. The process of setting the initial values or conditions for a system or program.

Step -2. Create an empty list with the purpose of storing the prospective candidates for cluster heads.

Step -3. For all the nodes in the network:

1. To establish a variable named maxConnectivity for the purpose of monitoring the greatest encountered connection value.
2. Declare and assign a variable named "selectedClusterHead" to hold the selected cluster head.
3. Perform an iterative process on each individual sensor node inside the given list.
4. If the battery level of the node is higher than or equal to the specified battery threshold (Bt), then continue to the subsequent step. Otherwise, exclude this particular node from further consideration.
5. In the event that the mobility of the node falls below the designated mobility threshold (Mt), it is appropriate to advance to the subsequent step. Conversely, if the node's mobility exceeds the threshold, it is advised to bypass this particular node.
6. The purpose of this inquiry is to do a connectivity check.
7. The connectivity value of the present node may be determined by enumerating the number of neighboring nodes that fall within its communication range.
8. If the value of connectivity is higher than or equal to the existing maximum connectivity, the maximum connectivity is updated and the current node is designated as the chosen candidate for the cluster head.

Algorithm 1 Secure WSN Cluster Head Selection based on Battery Level, Low Mobility, and Connectivity

The node designated as the selectedClusterHead candidate after the most recent iteration is selected as the cluster head in Algorithm 1. In the event that numerous nodes exhibit the same greatest degree of connection, it is advisable to prioritize the selection of the node with the most elevated battery level among them.

The output the Algorithm 1, consists of the node that has been recognized as the cluster head, based on criteria such as battery level, low mobility, and highest connection. Potential cluster head candidates are nodes that satisfy the characteristics of battery level, limited mobility, and connection. The ultimate choice is determined by the objective of optimizing connection and prioritizing better battery levels in the event of a tie. Connectivity is subject to several conditions, including signal strength, interference, and transmission range. The objective of this method is to identify a cluster head that is capable of ensuring consistent communication, while also optimizing energy consumption and avoiding the selection of nodes with high mobility as cluster heads. Prioritization is based on nodes that possess enough energy levels and have a robust network presence. The efficacy of the method is contingent upon precise parameter configurations and authentic mobility models. Now the routing using this cluster head must be secure and that is ensured using the second part of this proposed method.

4.2. Secure Selective Routing

Secondly, the secure selection of the cluster head process is furnished here. In the realm of Wireless Sensor Networks

RESEARCH ARTICLE

(WSNs), ensuring robust security is paramount. Effective cluster head selection plays a pivotal role in this endeavor. By identifying optimal cluster heads equipped with strong cryptographic capabilities, the network gains resilience against malicious attacks, guaranteeing data integrity and confidentiality in the WSN ecosystem.

Now assuming that network is running multiple independent processes and the collection is identified as PR[ ], where each process can be identified as P_i. This can be furnished for n number of processes denoted by equation (8).

$$PR[\,] = [P_1, P_2, \ldots . P_n] \quad (8)$$

Again, each process is associated with a single or multiple nodes. This can be formulated by equation (9).

$$P_i \leftrightarrow N_i \quad (9)$$

And each node is associated with the data in the network. This can be formulated by equation (10),

$$N_i \leftrightarrow D_i \quad (10)$$

Thus, together, it is denoted by equation (11).

$$P_i \leftrightarrow N_i \leftrightarrow D_i \quad (11)$$

As the associated datasets are extracted for each process and each node, it is straightforward to extract the security features on each data item. Such as, encryption algorithm (EA), rating of the encryption algorithm (EAR) and integrity of the data (DA). These security features are clear evidence of the routing security of the network. Assuming that, R is the rating of the routing security for each selected cluster head, thus this can be formulated by the equation (12).

$$R[\,] = \lambda \int \left(N_{CH[i].EA}, N_{CH[i].EAR}, N_{CH[i].DA}\right) \quad (11)$$

Assuming that λ is the arbitrary function to extract the above-mentioned features.

Finally, the nodes with the best features must be selected as cluster head, N_{CH}, this can be formulated by the equation (13).

$$N_{CH} = \prod_{Best\{R[\,]\}} N_{CH}[\,] \quad (13)$$

Further, based on the proposed analogy, secure routing with selective cluster heads is designed and furnished here in Algorithm 2.

Inputs:

- List of sensor nodes with their attributes (battery level, mobility, connectivity).
- Selected cluster head from the previous algorithm.
- Security ratings for each node based on security attributes.
- Routing table with connectivity information between nodes.

Output:

- Secure route from source node to the selected cluster head.

Assumption:

- Security attributes include encryption capability, authentication level, and intrusion detection capability.
- Security ratings are normalized values between 0 and 1, where higher values represent better security.

Process:

Step - 1. Create an empty list with the purpose of storing the secure route. (7)

Step - 2. The variables for the source node (Src) and the chosen cluster head (CH) are initialized. (8)

Step - 3. The verification process involves confirming the presence and functionality of the source node inside the network. (9)

Step - 4. The assignment involves the assessment and assignment of security ratings. (10)

Step - 5. The task at hand involves the assignment of security ratings to all nodes, which will be determined based on their respective security properties, including encryption, authentication, and intrusion detection. The presence of enhanced security features is positively correlated with elevated security ratings.

Step - 6. The identification of secure neighbors of the source node may be achieved by applying a filtering process to nodes that possess security ratings over a predetermined threshold.

Step - 7. Select the neighboring node with the most elevated security grade to serve as the subsequent intermediary in the routing process.

Step - 8. The objective is to establish a path from the source node to the chosen cluster head, using the secure neighbor as an intermediate node. (12)

Step - 9. The source node should be updated to function as the secure neighbor, and the process of repeating step 4 should continue until the secure route has been established to the cluster head.

Step - 10. It is essential to use suitable security techniques to encrypt and authenticate the communication between nodes along the secure path.

Step - 11. If the nodes possess intrusion detection capacity, they should be used to monitor and identify any abnormal or suspicious behavior occurring along the secure path. Implement appropriate remedial

RESEARCH ARTICLE

measures in response to the identification of abnormalities.

Step - 12. The output of the system is a list of nodes that constitute the secure path from the source node to the chosen cluster head.

Algorithm 2 Secure Routing using Selected Cluster Head and Security Rating

The determination of security ratings is predicated upon the evaluation of security features possessed by individual nodes, with the objective of prioritizing routing for nodes exhibiting superior security capabilities. The technique operates on the assumption that nodes possess up-to-date routing tables including information about connectivity and security aspects. The algorithm 2 places a higher emphasis on security compared to other considerations when selecting routes. Its primary objective is to construct a communication channel that is safe, while also taking into account the possibility of security breaches via the use of intrusion detection mechanisms. The security protocols and processes inside the WSN environment determine the security measures used during communication. The method presented in this study improves upon the cluster head-based routing approach by including the security features of individual nodes. The objective of this approach is to construct a reliable pathway from the originating node to the designated cluster head, with a focus on nodes that possess better security ratings. Additionally, it attempts to ensure the continuity of secure communication along the established path. The efficacy of the algorithm is contingent upon the precise evaluation of security attributes and the execution of suitable security protocols.

5. RESULTS AND DISCUSSIONS

The evaluation comprises several crucial facets, providing insight into the efficacy and execution of the plan in practical scenarios. The analysis starts by closely examining the dataset used, with the objective of gaining insights into its attributes and its pertinence to the research. Following this, an examination is conducted to determine the suitability of the developed routing strategy for the given dataset. This analysis aims to clarify how the design of the strategy corresponds to the characteristics and fluctuations of the dataset. This paper presents a comprehensive analysis of the cluster head selection process, focusing on its flexibility and stability across the network's lifespan. In the subsequent study, the evaluation of the packet delivery ratio examines the communication efficiency of the strategy by analyzing the proportion of packets that were successfully delivered out of the total number of packets sent. The study of energy consumption examines the influence of the strategy on the usage of power by nodes, which is essential for ensuring the long-term sustainability of the network. The examination of cluster lifetime and network lifetime further investigates the effectiveness of the technique in extending the duration of both individual clusters and the entire network functioning. Finally, a thorough examination of the security rating analysis reveals how the technique improves network security by assessing the security properties of nodes. The synthesis of these evaluations offers a full comprehension of the strategy's overall performance, its advantages, and opportunities for prospective improvement.

5.1. Dataset Analysis

Firstly, the utilized datasets are analyzed here in Table 2.

Table 2 Dataset Analysis

Dataset Name	Number of Nodes	Number of Parameters	Security Analysis	Routing Analysis
WSN Data [32], 2020	100	12	Yes	No
WSN Data [33], 2019	80	11	Yes	Yes
WSN-DS [34], 2022	85	9	Yes	Yes

The results are visualized graphically in Figure 1.

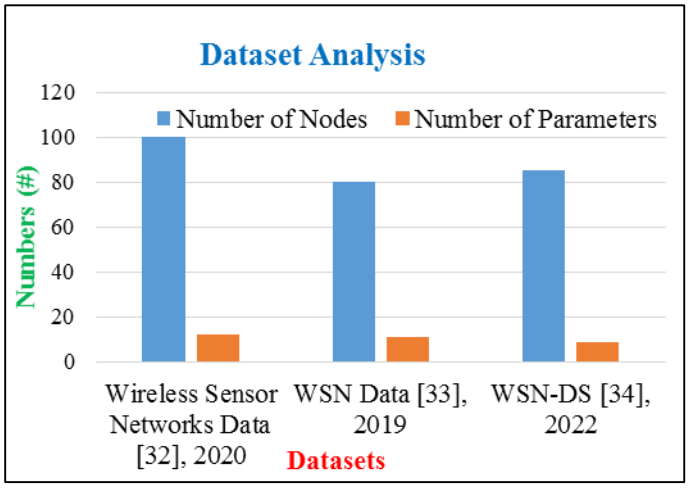

Figure 1 Dataset Analysis

The utilized datasets provide a unique and valuable contribution as a specialized resource for cluster head selection and secure routing detection systems in the context of wireless sensor networks. The primary characteristic of this system is its ability to provide a wide range of network circumstances that mimic real-world situations. These features allow for the effective training and assessment of proposed

RESEARCH ARTICLE

algorithms specifically designed for the complexities of wireless sensor network (WSN) settings

5.2. Applicability on Dataset

Secondly, the existing systems and the proposed method are evaluated on proposed datasets to evaluate the applicability of the dataset for better design of desired outcomes [Table 3].

Table 3 Applicability on Dataset

Author, Year	WSN Data [32], 2020	WSN Data, [33], 2019	WSN-DS [34], 2022
Ahutu et al. [5], 2020	√	√	√
Alotaibi et al. [7], 2021	√	√	√
Bin-Yahya et al. [8], 2022	√	√	
Chatterjee et al. [10], 2021	√	√	√
Fu et al. [12], 2021	√		
Haseeb et al. [15], 2020		√	
Pathak et al. [22], 2022		√	√
Verma et al. [29], 2022	√	√	√
Proposed Method	√	√	√

Hence, it is natural to realize that the proposed system has the functionalities to handle more diversified features.

5.3. Iteration-Wise Cluster Head Selection

Table 4 Iteration-Wise Cluster Head Selection

Iteration (#)	Number of Cluster Heads, at the end of the iteration		
	WSN Data [32], 2020	WSN Data, [33], 2019	WSN-DS [34], 2022
1	34	22	26
2	28	18	25
3	21	14	24
4	19	13	23
5	10	11	16
6	2	3	2
7	2	2	2
8	2	1	1
9	1	1	1
10	1	1	1

Thirdly, the cluster head selection outcomes are simulated on various datasets and the outcomes are furnished in Table 4. The simulation is performed over 100 simulations; however, the mean outcomes are listed here.

The outcomes are visualized graphically in Figure 2.

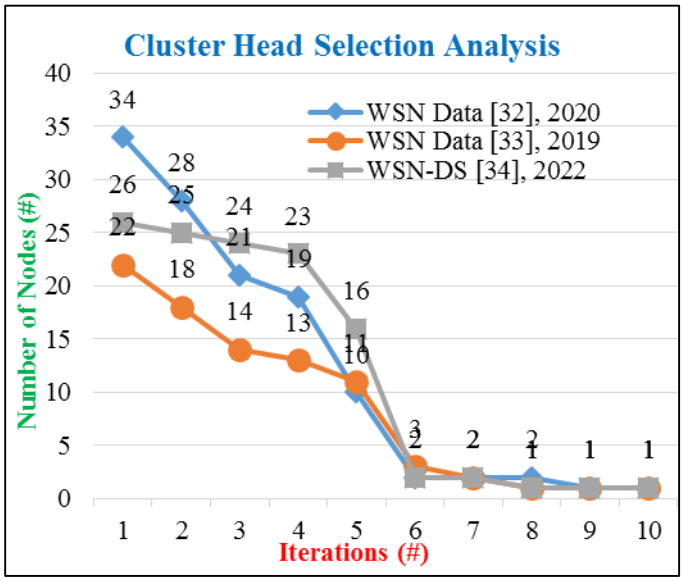

Figure 2 Cluster Head Selection

It is natural to realize that the selection of the cluster heads is fairly normalized in all the datasets. The optimal number of cluster heads are selected in maximum 4 to 6 iterations.

Also, the time taken on dataset to identify the optimal number of cluster heads are recorded and furnished in Table 5.

Table 5 Cluster Head Selection Time

Dataset	Number of Iterations	Optimal Number of Cluster Heads	Selection Time (ms)
WSN Data [32], 2020	6	2	2.788
WSN Data, [33], 2019	6	3	2.487
WSN-DS [34], 2022	6	2	4.074

The outcomes are visualized graphically in Figure 3.

The proposed method accelerates the process of selecting cluster heads by integrating power awareness and security factors. The technique effectively discovers nodes with ideal energy levels for leadership positions by using power awareness. The security-oriented approach of the system

RESEARCH ARTICLE

improves the process by considering the security ratings of nodes, so assuring the prompt selection of reliable cluster chiefs. The synergy optimizes the cluster head selection process by reducing the number of selection rounds. This results in an accelerated procedure while ensuring the health and security of the network are maintained.

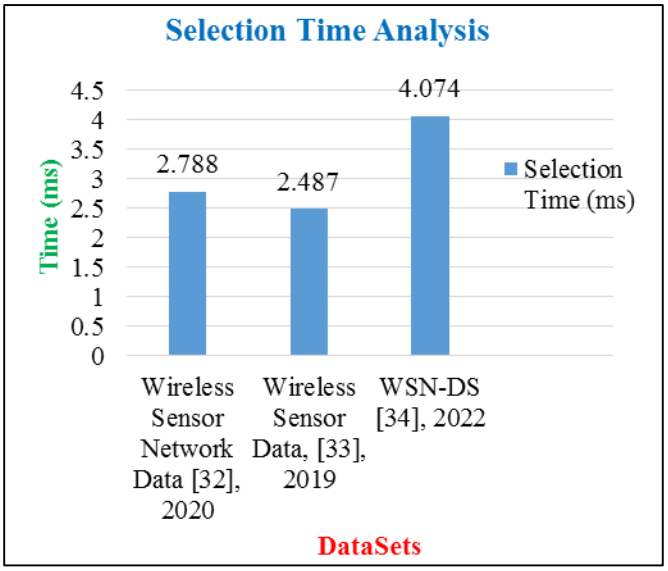

Figure 3 Cluster Head Selection Time Analysis

5.4. Packet Delivery Ratio Analysis

Fourthly, the packet delivery ratio is recorded during the simulation process. Also, the related works are simulated on the proposed datasets and the outcomes are compared in Table 6.

Table 6 Packet Delivery Ration Analysis

Author, Year	WSN Data [32], 2020	WSN Data, [33], 2019	WSN-DS [34], 2022
Ahutu et al. [5], 2020	82.07	84.37	80.63
Alotaibi et al. [7], 2021	82.89	86.06	81.44
Chatterjee et al. [10], 2021	86.21	89.50	83.88
Verma et al. [29], 2022	90.5	93.08	88.07
Proposed Method	96.85	98.66	93.36

The proposed system excels in improving the packet delivery ratio because of its combined focus on energy economy and security. The technique effectively addresses the issues of packet loss and route failures by carefully choosing energy-efficient pathways and dependable cluster heads. The incorporation of security features in this technique enhances the reliability and resilience of routing mechanisms, hence increasing the overall efficiency of packet delivery in wireless sensor networks.

The obtained results are visualized graphically in Figure 4.

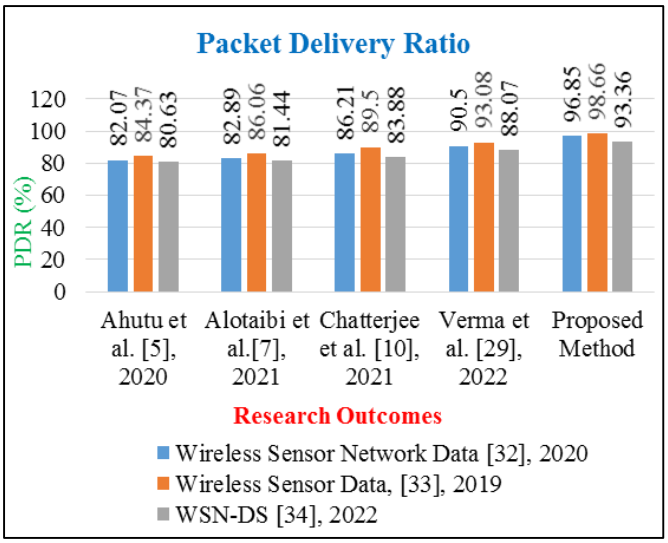

Figure 4 Packet Delivery Ratio

5.5. Energy Consumption Analysis

Fifth, the energy consumption for the proposed method and the existing systems are observed and recorded. For any secured routing algorithms, the energy consumption is expected to be higher, however, the proposed system has significantly demonstrated the improvement over other parallel algorithms. The results are displayed here in Table 7.

Table 7 Energy Consumption Analysis

Author, Year	WSN Data [32], 2020	WSN Data, [33], 2019	WSN-DS [34], 2022
Ahutu et al. [5], 2020	13.00	14.00	15.00
Alotaibi et al. [7], 2021	13.00	11.00	13.00
Chatterjee et al. [10], 2021	11.00	13.00	15.00
Verma et al. [29], 2022	10.00	14.00	16.00
Proposed Method	0.70	11.00	12.20

The proposed method is considered a better strategy for managing energy usage owing to its comprehensive and

RESEARCH ARTICLE

integrated methodology. The technique enhances routing patterns by including power awareness, resulting in reduced energy consumption and increased longevity of nodes. Concurrently, the security-conscious choices of the system guarantee the efficient use of energy by preventing any wastage on compromised nodes. The integration of energy efficiency and security ensures optimal usage of energy, making the approach particularly successful in minimizing total energy consumption in the wireless sensor network.

The results are observed visually here in Figure 5.

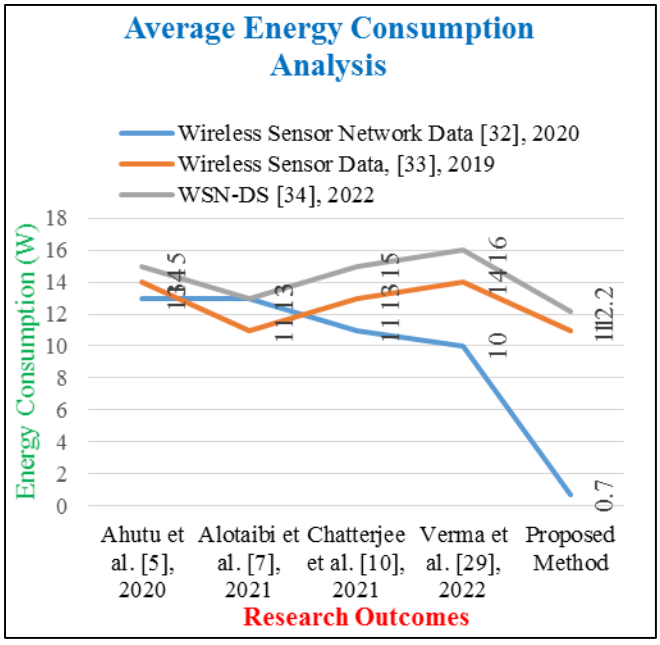

Figure 5 Average Energy Consumption Analysis

5.6. Network Lifetime Analysis

Sixth, improving the cluster and also the overall network lifetime is the prime importance for any routing algorithm. The outcome from the simulation is recorded for the proposed and the existing systems, which are furnished here in Table 8.

Table 8 Network Lifetime Analysis

Author, Year	WSN Data [32], 2020	WSN Data, [33], 2019	WSN-DS [34], 2022
Ahutu et al. [5], 2020	93	90	80
Alotaibi et al. [7], 2021	89	86	93
Chatterjee et al. [10], 2021	80	86	87
Verma et al. [29], 2022	93	84	94
Proposed Method	110	121	97

The proposed method demonstrates the superiority of this approach in improving the overall lifespan of the network. This is achieved by a combined emphasis on both energy efficiency and security considerations. The proposed technique aims to enhance the operational lifespan of the network by carefully choosing energy-efficient routes and reliable cluster heads. This approach effectively increases the individual node lives, hence lengthening the overall network's operational span. The incorporation of security ratings serves to enhance the effective allocation of energy resources among reliable nodes, hence bolstering the long-term sustainability of the network. The complete nature of this technique renders the concept very proficient in enhancing the total lifespan of wireless sensor networks.

The outcomes are also visualized graphically in Figure 6.

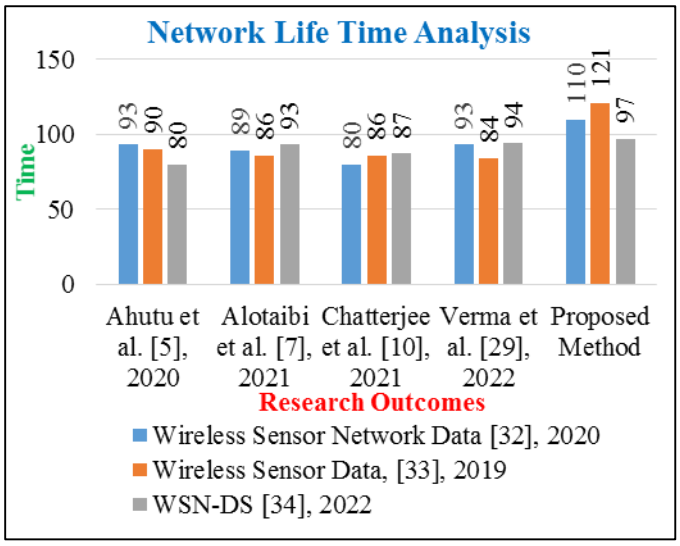

Figure 6 Network Lifetime Analysis

5.7. Security Rating Analysis

During the final phase of analysis, it is important to build the final ratings of the security measures. The security rating is derived from the parameters such as rating of the cryptography algorithm, data integrity and others. The obtained results are furnished here in Table 9.

The proposed strategy demonstrates enhanced security capabilities as a result of its comprehensive incorporation of security issues. The technique evaluates the encryption capabilities, authentication levels, and intrusion detection possibilities of nodes in order to issue security ratings that accurately represent their degree of trustworthiness. The purpose of this focused assessment is to enhance the security properties of cluster heads and routing pathways by including nodes with strong security capabilities. As a consequence, the strategy's focus on security qualities enhances the overall

RESEARCH ARTICLE

security stance of the network, leading to increased and more dependable security ratings.

Table 9 Security Rating Analysis

Author, Year	WSN Data [32], 2020	WSN Data, [33], 2019	WSN-DS [34], 2022
Ahutu et al. [5], 2020	0.410	0.336	0.143
Alotaibi et al. [8], 2021	0.367	0.474	0.402
Chatterjee et al. [10], 2021	0.480	0.347	0.392
Verma et al. [29], 2022	0.439	0.323	0.170
Proposed Method	0.854	0.598	0.901

6. COMPARATIVE ANALYSIS

The Secure Power Aware Hybrid Routing Strategy for Wireless Sensor Networks demonstrates a clear advantage when compared to traditional routing algorithms. In contrast to conventional approaches that tend to prioritize either energy optimization or security issues in isolation, our hybrid technique effectively combines and harmonizes both elements. The comparative analysis is furnished here in Table 10.

It is natural to realize that the proposed method has surpluses the recent research. The proposed technique effectively enhances network performance by simultaneously addressing energy efficiency via optimum routing pathways and security improvement through rigorous security attribute assessments. The iterative method of selecting cluster heads incorporates power-awareness to efficiently pick leaders that optimize energy consumption. Additionally, the incorporation of security ratings guarantees the development of reliable pathways. The presence of this duality leads to enhanced rates of packet delivery, decreased energy consumption, and extended lifespans of both the network and its clusters. The "Secure Power Aware Hybrid Routing Strategy for WSN" is a noteworthy solution that combines energy efficiency and security qualities, distinguishing it from single-focused techniques. This amalgamation enables the strategy to optimize network resilience, resource consumption, and overall operational efficiency.

Table 10 Comparative Analysis on All Datasets

Author, Year	Mean Iterations for CH Selection	Mean Packet Delivery Ratio (%)	Mean Energy Consumption (W)	Network Lifetime (Rounds)	Security Rating
Ahutu et al. [5], 2020	12	70.03	13.29	95	0.413
Alotaibi et al. [7], 2021	14	78.92	11.59	84	0.513
Yahya et al. [8], 2022	14	76.19	11.45	82	0.594
Chaterjee et al. [10], 2021	10	75.16	10.89	67	0.513
Fu et al. [12], 2021	13	70.08	10.41	62	0.461
Haseeb et al. [15], 2020	13	79.12	12.84	71	0.418
Pathak et al. [22], 2022	15	77.58	10.13	76	0.507
Verma et al. [29], 2022	12	74.97	10.87	97	0.573
Proposed Method	6	98.02	10	116	0.854

7. CONCLUSION

In summary, the study findings provide a thorough assessment of several routing approaches for wireless sensor networks (WSNs) by considering average iterations for cluster head selection, average packet delivery ratio, average energy consumption, network lifespan, and security ratings. Nevertheless, the "Secure Power Aware Hybrid Routing Strategy for Wireless Sensor Networks" outperformed all other approaches. The cluster head selection process achieved a lower mean of 6 iterations, surpassing the performance of other methods in terms of packet delivery ratio (98.02%) and mean energy usage (10 W). Additionally, it demonstrated impressive endurance with a network lifespan of 116 rounds. Furthermore, the implemented technique demonstrated a commendable security grade of 0.854, so highlighting its efficacy in preserving the integrity of the network. The

RESEARCH ARTICLE

aggregated study results highlight the dominance of the suggested hybrid approach, which successfully integrates energy efficiency and security to improve the performance of Wireless Sensor Networks (WSNs) across several crucial aspects.

REFERENCES

[1] M. E. Al-Sadoon, A. Jedidi and H. Al-Raweshidy, "Dual-Tier Cluster-Based Routing in Mobile Wireless Sensor Network for IoT Application," in IEEE Access, vol. 11, pp. 4079-4094, 2023, doi: 10.1109/ACCESS.2023.3235200.

[2] Chowdhuri, R., Barma, M.K.D. Node position estimation based on optimal clustering and detection of coverage hole in wireless sensor networks using hybrid deep reinforcement learning. J Supercomput 79, 20845–20877 (2023). https://doi.org/10.1007/s11227-023-05494-8.

[3] Han D, Du X, Wang L, Liu X, Tian X. Trust-Aware and Fuzzy Logic-Based Reliable Layering Routing Protocol for Underwater Acoustic Networks. Sensors. 2023; 23(23):9323. https://doi.org/10.3390/s23239323.

[4] Sirajuddin, M. ., & Kumar, B. S. . (2023). Intelligent Secure and Malicious-Free Route Management Strategy for IoT-based Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 369–380. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2962

[5] Ahutu, O. R., & El-Ocla, H. (2020). Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks. IEEE Access, 8, 63270–63282. https://doi.org/10.1109/ACCESS.2020.2983438

[6] Alghamdi, T. A. (2018). Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method. IEEE Access, 6, 53576–53582. https://doi.org/10.1109/ACCESS.2018.2865909

[7] Alotaibi, M. (2021). Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN. IEEE Access, 9, 159187–159197. https://doi.org/10.1109/ACCESS.2021.3130005

[8] Bin-Yahya, M., Alhussein, O., & Shen, X. (2022). Securing Software-Defined WSNs Communication via Trust Management. IEEE Internet of Things Journal, 9(22), 22230–22245. https://doi.org/10.1109/JIOT.2021.3102578

[9] Bin-Yahya, M., & Shen, X. (2023). Secure and Energy-Efficient Network Topology Obfuscation for Software-Defined WSNs. IEEE Internet of Things Journal, 10(3), 2031–2045. https://doi.org/10.1109/JIOT.2022.3144873

[10] Chatterjee, T., Karmakar, S., & Das Bit, S. (2021). IPLQueeN: Integrity Preserving Low-Overhead Query Handling Over NDN-Based WSN. IEEE Access, 9, 82786–82811. https://doi.org/10.1109/ACCESS.2021.3086460

[11] Feng, W., Wang, F., Xu, D., Yao, Y., Xu, X., Jiang, X., & Zhao, M. (2020). Joint Energy-Saving Scheduling and Secure Routing for Critical Event Reporting in Wireless Sensor Networks. IEEE Access, 8, 53281–53292. https://doi.org/10.1109/ACCESS.2020.2981115

[12] Fu, X., Yang, Y., & Postolache, O. (2021). Sustainable Multipath Routing Protocol for Multi-Sink Wireless Sensor Networks in Harsh Environments. IEEE Transactions on Sustainable Computing, 6(1), 168–181. https://doi.org/10.1109/TSUSC.2020.2976096

[13] Ganesh, S., & Amutha, R. (2013). Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. Journal of Communications and Networks, 15(4), 422–429. https://doi.org/10.1109/JCN.2013.000073

[14] Gope, P., Lee, J., & Quek, T. Q. S. (2017). Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks. IEEE Sensors Journal, 17(2), 498–503. https://doi.org/10.1109/JSEN.2016.2628413

[15] Haseeb, K., Almustafa, K. M., Jan, Z., Saba, T., & Tariq, U. (2020). Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network. IEEE Access, 8, 163962–163974. https://doi.org/10.1109/ACCESS.2020.3022285

[16] Haseeb, K., Islam, N., Almogren, A., & Ud Din, I. (2019). Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things. IEEE Access, 7, 185496–185505. https://doi.org/10.1109/ACCESS.2019.2960633

[17] Haseeb, K., Islam, N., Almogren, A., Ud Din, I., Almajed, H. N., & Guizani, N. (2019). Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs. IEEE Access, 7, 79980–79988. https://doi.org/10.1109/ACCESS.2019.2922971

[18] Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2017). SCOTRES: Secure Routing for IoT and CPS. IEEE Internet of Things Journal, 4(6), 2129–2141. https://doi.org/10.1109/JIOT.2017.2752801

[19] Li, S., Zhao, S., Wang, X., Zhang, K., & Li, L. (2014). Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks. IEEE Systems Journal, 8(3), 858–867. https://doi.org/10.1109/JSYST.2013.2260626

[20] Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013–2027. https://doi.org/10.1109/TIFS.2016.2570740

[21] Mutalemwa, L. C., & Shin, S. (2021). Novel Approaches to Realize the Reliability of Location Privacy Protocols in Monitoring Wireless Networks. IEEE Access, 9, 104820–104836. https://doi.org/10.1109/ACCESS.2021.3099499

[22] Pathak, A., Al-Anbagi, I., & Hamilton, H. J. (2022). An Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs. IEEE Internet of Things Journal, 9(23), 23826–23840. https://doi.org/10.1109/JIOT.2022.3189832

[23] Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J., & Ding, Q. (2017). Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network. IEEE Access, 5, 9599–9609. https://doi.org/10.1109/ACCESS.2017.2706973

[24] Rathee, M., Kumar, S., Gandomi, A. H., Dilip, K., Balusamy, B., & Patan, R. (2021). Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks. IEEE Transactions on Engineering Management, 68(1), 170–182. https://doi.org/10.1109/TEM.2019.2953889

[25] Roy, S., Conti, M., Setia, S., & Jajodia, S. (2014). Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact. IEEE Transactions on Information Forensics and Security, 9(4), 681–694. https://doi.org/10.1109/TIFS.2014.2307197

[26] Saleem, K., Fisal, N., & Al-Muhtadi, J. (2014). Empirical Studies of Bio-Inspired Self-Organized Secure Autonomous Routing Protocol. IEEE Sensors Journal, 14(7), 2232–2239. https://doi.org/10.1109/JSEN.2014.2308725

[27] Salim, A., Osamy, W., Khedr, A. M., Aziz, A., & Abdel-Mageed, M. (2021). A Secure Data Gathering Scheme Based on Properties of Primes and Compressive Sensing for IoT-Based WSNs. IEEE Sensors Journal, 21(4), 5553–5571. https://doi.org/10.1109/JSEN.2020.3032585

[28] Selcuk Uluagac, A., Beyah, R. A., & Copeland, J. A. (2013). Secure SOurce-BAsed Loose Synchronization (SOBAS) for Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 24(4), 803–813. https://doi.org/10.1109/TPDS.2012.170

[29] Verma, S., Zeadally, S., Kaur, S., & Sharma, A. K. (2022). Intelligent and Secure Clustering in Wireless Sensor Network (WSN)-Based Intelligent Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 23(8), 13473–13481. https://doi.org/10.1109/TITS.2021.3124730

[30] R. Alkanhel, K. Chinnthambi, C. Thilagavathi, An energy-efficient multi-swarm optimization in wireless sensor networks, Intelligent Automation & soft computing IASC 36 (2) (2023), https://doi.org/10.32604/iasc.2023.033430.

[31] D. S. Misbha, ''Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model,'' High-Confidence Comput., vol. 3, no. 2, Jun. 2023, Art. no. 100126, doi: 10.1016/j.hcc.2023.100126.

RESEARCH ARTICLE

[32] Wireless Sensor Network Data, Kaggle, https://www.kaggle.com/datasets/halimedogan/wireless-sensor-network-data, (Accessed on 07-07-2023)
[33] Wireless sensor data, Kaggle, https://www.kaggle.com/datasets/paulopinheiro/wireless-sensor-data, (Accessed on 07-07-2023)
[34] WSN-DS: A dataset for intrusion detection systems in wireless sensor networks, Kaggle, https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds, (Accessed on 07-07-2023).

Authors

Mohammad Sirajuddin, is a Research Scholar, CSE, Jawaharlal Technological University Hyderabad, Telangana, India. His current Research interest includes Wireless Sensor Networks, Machine Learning, IoT, and Artificial Intelligence. He has published many refereed academic papers/ articles in SCI and Scopus indexed journals. He received training on Advanced Machine Learning Algorithms, Internet of Things and Mission 10X. He attended conferences and published papers in reputed journals like Springer, IEEE.

Dr. B. Sateesh Kumar, is a Professor of Computer Science & Engineering, Jawaharlal Nehru Technological University Hyderabad, College Of Engineering Jagitial (JNTUHCEJ)Telangana, India. He is the recipient of many national and international awards including Compliments for Training in JAVA programming, TASK - Telangana, 2016, The Vishista Seva Puraskar, JNTUHCEJ, 2011, Bharath Jyoti Award, IIFS Delhi, 2011, Best Teacher Award, JBREC, 2006 for Outstanding Services, Achievements, Contributions, Meritorious Services, Outstanding Performance and Remarkable Role in the field of Education and Services. He Organized a FDP on Advanced Machine Learning Algorithms, JNTUH HRDC, 20-09-2021 to 25-09-2021. He received training on Big Data and cloud Analytics and Data Mining and Data Warehouse techniques. He served/is serving as a Governing Body Member to the Boards of studies of various Universities. He also served as Kakatiya University Board of Studies in Computer Science (PG and UG) as External Member from Feb-2020 to Feb-2022. Professional and service-oriented organizations, including the Indian Society for Technical Education, have accepted him as a member / life member (ISTE).2022. Professional and service-oriented organizations, including the Indian Society for Technical Education, have accepted him as a member / life member (ISTE).

How to cite this article:

Mohammad Sirajuddin, B. Sateesh Kumar, "Secure Power Aware Hybrid Routing Strategy for Large-Scale Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 10(6), PP: 1015-1029, 2023, DOI: 10.22247/ijcna/2023/223695.