International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I11P126

Volume 72 Issue 11, 257-268, November 2024

Original Article

An Investigation on Energy-Aware Secured Clustering Algorithm for Wireless Sensor Networks

Natraj N. A.[1*], Giri G. Hallur[1], Prasanna Kulkarni[1], Tripti Dhote[1], Gopinath S[2]

[1]*Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, India.*
[2]*Department of ECE, Karpagam Institute of Technology, Coimbatore, India.*

[*]*Corresponding Author : natraj@sidtm.edu.in*

Received: 14 August 2024 Revised: 20 October 2024 Accepted: 29 October 2024 Published: 29 November 2024

Abstract *- Wireless Sensor Networks (WSN) are known for their extensive applications in the monitoring process. The future IoT will be dependent on WSN, which is made of WSN nodes. The major issues of WSN are energy efficiency and security. Efficient clustering and integration of security measures in the sensor nodes can overcome those major issues. In this research an Energy Conscious Secured Clustering Algorithm (ECSCA) is proposed to overcome the mentioned issues. The proposed method considers different factors like residual energy, degree of reachability of the sensor node, and cluster head supremacy for efficient cluster formation. After the cluster formation process, the node to node communication should be secured to prevent attacks from the malicious nodes in the network. The proposed method ensures communication by integrating an Elliptic Curve Cryptography (ECC) based security mechanism with the clustering process. The simulation results are analyzed using the existing Secured Localization Routing Protocol (SLRP) scheme and different metrics like packet delay, location accuracy, and Malignant Node Identification Ratio (MNIR). The results proved to be more efficient than the existing scheme.*

Keywords *- WSNs, Energy ECSCA, ECC, Clustering, Security, Cryptography, ECC.*

1. Introduction

A Wireless Sensor Network (WSN) uses tiny, battery-powered sensors to detect and send data wirelessly. Sensor nodes are scattered across a vast region and may be used for environmental monitoring, tracking people or objects, and managing industrial operations. WSNs are distinguished by their ability to operate in harsh environments, low power consumption, and self-organization and adaptability to changing conditions. They have become increasingly popular due to advances in wireless communication, sensor technology, and miniaturization. WSN sensor nodes need batteries, restricting communication and computation energy. Nodes may fail, and network lifespan decline. Wireless communication channels used by sensor nodes have limited bandwidth, which can cause congestion and increased latency. Sensor nodes in a WSN are frequently deployed in harsh environments, such as industrial plants or remote locations, resulting in high temperatures, vibration, and dust and moisture exposure. Eavesdropping, jamming, and node capture are all security attacks that can be used against WSNs. The scalability issue of sensor nodes can be termed as, if there is any surge in the number of nodes in a network, it becomes more challenging to manage and control the network, potentially resulting in scalability issues. The QoS requirements in many WSN applications are very strict, and they include low delay, high throughput, low power consumption, and high reliability. Many WSNs are designed to self-organize, which means that sensor nodes discover and join the network, configure themselves, and adapt to changing conditions. However, this can result in problems like network partitioning and unreliable communication. Because of the dynamic and harsh environment, limited resources, and the need to balance energy consumption with performance, routing in WSNs is a difficult task. WSNs are known for their role in a variety of applications in recent years, attracting the interest of academics due to their complicated, multifarious needs, which frequently reveal inherent trade-offs. It is made up of individual sensor nodes that are linked together via adhoc and self-configuring connections. Based on the kind of application, wireless sensor networks are classed as pre-determinate or unsupervised networks. The benefits include Quality of Service (QoS), tolerance of faults, scalability, and resilience obtained by the pre-determinate network type. Human monitoring for sensor networks is constrained or disallowed in many pragmatic circumstances since nodes are distributed in key areas such as interior parts of rainforests and submerged habitats. These are unmonitored networks. Environmental wireless sensor nodes measure many properties. Wireless Sensor Networks (WSN) cluster sensor nodes to improve network performance and energy efficiency. The Cluster Head (CH) of a clustered Wireless Sensor Network (WSN) manages the cluster's nodes. Clustering

breaks the network into smaller sub-networks that monitor certain areas or metrics. By partitioning the network, CHs may reduce communication and computation, improving energy saving and network performance. A clustering of wireless sensor nodes is required for effective monitoring. Sensor networks benefit from the clustering of nodes in a number of ways. Clustering contributes to congestion-free network traffic, scalable networking, and robustness.

The clustering of wireless sensor nodes involves different procedures. The clustering of nodes ensures localizations through various mechanisms. The nodes in networks are scarcely distributed, and this ensures advantages in aspects like scalability, data gathering efficiency, and enhanced power consumption.

The clusters will transmit information to the sink nodes via the cluster heads. The nodes constitute the members of the cluster network. The nodes transmit the compiled data to the cluster chiefs. Clustering algorithms of various types can be used in WSNs, each with its advantages and disadvantages.

Clustering algorithms are built to be adaptable to the dynamic nature of WSNs, which means they can reconfigure themselves as the network changes. Clustering, on the other hand, can add complexity and management challenges, such as determining the optimal number of clusters and choosing appropriate CHs. Some popular clustering algorithms include:

- LEACH [9] (reference) alternates Cluster Head roles across network nodes. This stabilizes node energy usage and extends network life.
- PEGASIS [14] (reference) uses a chain-like structure to transport data from sensor nodes to the sink. Energy usage is reduced by sending data from the nearest node to the next.
- HEED [14] (reference) algorithm (Hybrid Energy-Efficient Distributed Clustering): This algorithm is a cross between LEACH and PEGASIS, attempting to combine the benefits of both algorithms to improve energy efficiency and network lifetime. A widely used clustering approach is the LEACH [18] Protocol. It is a protocol in which the major number of nodes broadcast data to the Cluster Head (CH). Before sending the data to the sink, these CHs combine and compress the data. Every node has a radio based on LEACH that can communicate directly with the base node station or the closest cluster head; however, it is wasteful to utilize this radio continuously and at full power. Though LEACH is advantageous and traditional, it has drawbacks, which are listed below.
- Limited scalability: LEACH is designed for small-scale networks and may not be suitable for more extensive networks with many nodes.
- High control overhead: The LEACH algorithm requires a significant amount of control overhead to manage the cluster formation and to elect the cluster heads. This can lead to an increase in energy consumption and reduce network performance.
- Load imbalance: In LEACH, the load is not evenly distributed among the cluster heads, which can lead to some cluster heads running out of energy faster than others.
- High energy consumption: High control overhead and load imbalance in LEACH cause energy consumption to be lower than expected.
- Static threshold: The threshold for becoming a cluster head is fixed in the LEACH algorithm, which may not be suitable for all situations.
- Limited adaptability: The LEACH algorithm is not adaptable to changes in network conditions, such as changes in node density or traffic patterns, which can lead to suboptimal performance.

Cluster heads are not chosen according to their remaining energy levels. The random formation of clusters of varying sizes presents a significant challenge. Communication between cluster heads and base stations in a single hop results in decreased energy efficiency. The LEACH protocol is susceptible to various attacks, including HELLO flooding, selective forwarding, and Sybil attacks. These vulnerabilities result in performance issues such as packet loss, packet alteration, spoofing, and packet replaying. Wireless Sensor Networks (WSNs) are employed in various applications, including industrial process monitoring, environmental monitoring, and military surveillance. Given their extensive utilization and the sensitive data they gather, it is essential to guarantee that communication between nodes remains secure and safeguarded against unauthorized access. Secure routing in wireless sensor networks is essential to prevent unauthorized interception or alteration of transmitted data, as well as to maintain the normal functioning of the network. Secure routing enhances data privacy and integrity while offering authentication and access control mechanisms to prevent unauthorized network access. Cryptography can facilitate secure communication in Wireless Sensor Networks (WSNs). This process involves the application of mathematical algorithms for the encryption and decryption of information. It is utilized for secure communication and safeguarding sensitive information from unauthorized access. Cryptography consists of two primary stages: encryption and decryption. Encryption involves the transformation of the original message, known as plaintext, into an encoded message, referred to as ciphertext, utilizing a designated encryption algorithm and a confidential key. The decryption of the encoded message is contingent upon possession of the appropriate decryption key. The decryption process involves converting the encoded message back to its original form through the application of the decryption algorithm and the corresponding secret key. Symmetric-key and asymmetric-key encryption techniques exist. Symmetric-key algorithms encrypt and decode using one key.

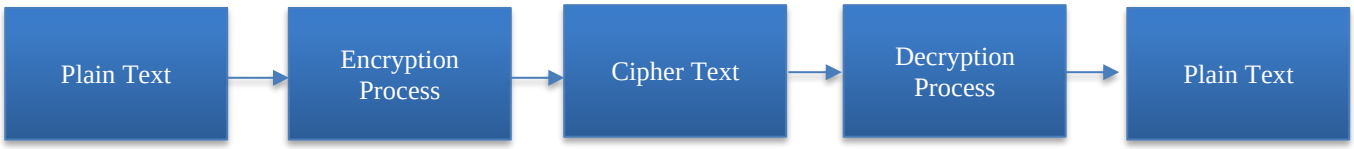

Fig. 1 Cryptography process

Asymmetric-key algorithms use two keys for encryption and decryption. The RSA algorithm is a popular asymmetric-key method that uses public and private keys. The private key decrypts, whereas the public key encrypts. The computational difficulty of factoring big prime integers secures RSA. Figure 1 illustrates the cryptography process. The first phase of the cryptography process involves generating a key or a pair of keys (public and private) designated for encryption and decryption. A key generation algorithm often produces a key. The security of the encryption process is intrinsically linked to the robustness of the key, underscoring the need to use a safe essential generation technique. After the generation of the key or keys, the subsequent step is to encrypt the plaintext (original message) using an encryption method and the key.

The encryption technique employs mathematical procedures to convert plaintext into ciphertext, rendering the message incomprehensible without the key. The encoded message (cipher text) is then transferred to the designated recipient over an unreliable route, such as the internet. The receiver of the encrypted communication uses the decryption algorithm and the key to decipher the ciphertext and get the original plaintext. Authentication is an optional procedure that may be used to verify that the message originated from the intended sender and is unaltered throughout transmission. On the other hand, several techniques can be used to protect the routing in WSNs, including:

- Encryption: Data can be encrypted before it is transmitted to prevent unauthorized access or tampering. This can be done using symmetric or asymmetric encryption algorithms, such as AES or RSA.
- Authentication: Sensor nodes can be required to authenticate themselves before they are allowed to participate in the network. This can be done using digital signatures, certificates, or other authentication protocols.
- Access control: Access to the network can be restricted by implementing access control mechanisms, such as firewalls or intrusion detection systems.
- Secure routing protocols: Routing protocols can be designed to be secure by including security features such as secure key distribution, route authentication, and secure routing table updates.
- Physical security: To protect the network from physical tampering, the sensor nodes can be located in secure locations or protected by tamper-proof enclosures.
- Trust management: Trust management schemes can be used to establish trust among the sensor nodes and protect the network from malicious nodes.

2. Literature Review

Natraj et al. proposed an SLRP method to attain the balance between secured location identification and energy efficiency. The authors used a 3-phase mechanism, which includes cluster formation, localization procedures and security phase [1]. While SLRP aims to balance secure location integrity and energy efficiency, the paper does not thoroughly discuss the potential trade-offs between these two aspects. Kim KhanhLe-Ngoc et al. proposed a Sugeno-based Fuzzy Logic Controller [2] based clustering algorithm. In this method, the cluster heads within the network gather the data from the nodes and forward them to one of the sinks.

This method also uses multi hop routing to forward the data to the destination. The proposed approach attempts to balance the load among sensor nodes, maximise network longevity, and reduce energy usage. The programme groups nodes into clusters using a fuzzy clustering technique and then utilises ISSA to optimise the placement of cluster heads. The ISSA algorithm is a meta-heuristic optimisation method that draws inspiration from squirrels' feeding habits. The authors concluded that their approach outperformed the other existing clustering mechanisms. The research does not consider the impact of network size on the performance of the proposed algorithm, and it may not be scalable for large networks.

Hosseinzadeh et al. developed the Cluster-Based Trusted Routing Framework (CTRF) [3], which uses the Fire Hawk Optimizer (FHO) to secure wireless sensor networks. CTRF's Weighted Trust Mechanism (WTM) uses exponential coefficients to dynamically modify trust levels depending on trust parameters, including reception rate, redundancy rate, and sensor node energy condition. CTRF uses FHO-based clustering to improve cluster head selection, considering energy and trust. The proposed clustering method uses an innovative cost function that incorporates the cluster head's location, energy, base station distance, and cluster size. CTRF also uses a trustworthy routing algorithm to build inter-cluster routing paths, assuring data privacy from cluster heads to the base station by considering power consumption, route quality, dependability, and total hop count.

Bhisham Sharma et. Al [4] analysed about the implantation of the Elliptical Curve Cryptography (ECC) for Wireless Sensor Networks. This paper also explored the hardware implementation of ECC Using Java Sunspot kit. The authors related the results with the further Public Key Asymmetric Cryptography methods and found them to be more efficient in terms of Key Size and Key Exchange than

the other PKI methods. The study offered insights into the theoretical underpinnings of ECC and its possible use in WSNs. However, it did not provide a detailed security analysis or performance assessment of the suggested system.

I.S. Akila et al. presented an Efficient Energy Harvesting Assisted Clustering in [5]. The proposed method is said to contribute effectively to forming clusters free from residual nodes and overlapping issues. The nodes were equipped with energy-harvesting devices. The authors proposed that there is a considerable reduction in the need for reclustering. Though the results proved to outperform traditional clustering schemes in terms of network lifetime and energy efficiency, they did not focus on secured communication between the nodes in the network.

The authors presented a security-oriented energy-efficient routing scheme [6] to improve wireless sensor node lifespan. Secure routing and energy optimization were recommended. Sensor nodes were notified of nearby node positions and energy levels. Two random walking routing algorithms find the quickest path to prevent jamming assaults. Protecting the network against jammer-induced packet flooding requires preventing this attack. Energy efficiency and security were the emphasis of this study. However, it failed to evaluate the proposed system across different network topologies, deployment scenarios, and application requirements.

Junqi Duan et al. [7] proposed a Secure Routing framework. This is based on the computation of trust and management technologies. This framework was used to design optimized routes to protect paths and nodes from attackers. The trust table of the source node is used to locate and identify neighbour nodes. The destination node obtains the data based on the node's localization information. This data is prevented from the attacker nodes. To meet the sensor network's reliability needs, a trust metric was added to each node's packet information. The authors could have addressed the research in terms of scalability and trust refining aspects.

In the article [8], the authors surveyed the different clustering mechanisms. The author outlined the four different clustering mechanisms: EAFCA, EEHC, EERC, and ADCA. Each method was designed for WSNs with a different perspective. The author disclosed that the performance of the proposed clustering approaches was efficient. The authors briefly introduced different clustering techniques without providing an in-depth analysis and comparison among them. A more comprehensive evaluation of the advantages, disadvantages, and performance characteristics of each clustering technique would be beneficial. Comparisons based on metrics such as energy efficiency, scalability, network lifetime, and data aggregation capability could have provided a better understanding of their suitability for different WSN applications.

Pooja Gulganwa and Saurabh Jain proposed an ML-based Centralized IDS for Energy efficiency in WSNs [9]. The authors said that the network cluster is created without distracting the default activity of the WSN. The ML models used were SVM and MLP in the proposed method. The result proved that detection accuracy was improved compared to the existing methods. The algorithm uses the k-means clustering technique to classify nodes into different clusters and assigns a weight to each node based on its residual energy.

The nodes with higher energy are selected as cluster heads to reduce energy consumption. The proposed algorithm also uses Elliptic Curve Cryptography (ECC) to provide secure communication between nodes. The limitation of this article is that the EES-WCA algorithm relies on the assumption that the residual energy of nodes accurately reflects their ability to perform cluster head duties effectively.

In article [10], the authors explored the LEACH Routing protocol for the WSNs. The authors explored cluster-based routing in the LEACH Protocol. They also explored the minimization of energy consumption through cluster-based routing protocol in LEACH protocol. They analysed the TDMA-based Media Access Control protocol in LEACH protocol. Though this article explored the usage of leach protocol in Wireless Sensor networks, it could have focused more on clustering and secure communication between the nodes. The research also lacks a comprehensive evaluation of its performance in realistic and dynamic WSN environments.

V. Vijayalakshmi et al. proposed a secured localization using ECC in WSNs [11]. The author's objective was to overcome the security problem in wireless sensor networks. The authors used Elliptic Curve Cryptography along with the TOA position scheme to implement security measures in WSNs effectively. The authors related the results with the other PKI cryptography methods and found them more effective.

In the article [12], the authors proposed an Optimized and secure routing through ECC in wireless sensor networks. The authors proposed security routing through a deep-learning approach. Through the Elliptic curve cryptography method, they proposed offering a secure routing mechanism. Multiple parameters were considered for performance analysis, and this method effectively offered secure routing. Celso Moraes and Dongsoo Har [13] employed charge to balance WSN clustering and energy. First, a mobile node charger was used to study sensor node energy transactions. In the first target phase level, the CH and maximum cluster members were charged. Paths were charged based on cluster area head distribution. The energy trading approach balanced energy use in the second stage during data loss and route failures.

Hong Fu et al. [14] proposed an AELAR Algorithm to find pathways that consume less energy from the source to the

destination node. There was a partitioned routing request zone, and the following hop node was determined using a choose equation. Nodes move across the network region at random. The stated expression and routing region can both be modified on the basis of node location. The routes are determined rapidly, and energy usage is lowered thanks to an adaptive process.

Hong Fu et al. [14] studied the maximum lifespan technique for tracking and monitoring a dynamic sensor node in a sensor field. The resources and challenges for detecting and transferring data between sensor nodes were discovered. Path blockage causes were also found to extend the network lifespan. An efficient motion method was also devised to track the localization information of sensor nodes. The shortest path technique was used to determine the location of sensor nodes and the transmission of information.

Firdozali and Nagamalar [18] proposed a Routing scheme based on an energy-aware mobile sink to decrease sensor node energy dissipation. This work measured and summarised the energy dissipation of sensor nodes. Node selection and energy reduction were effective in improving energy efficiency. To increase network spread, the mobility radius of the target node was evaluated. In some circumstances, static sink nodes are placed to enhance the level of energy regardless of the radius of the destination node mobility.

Table 1 gives a short review of the comparison of various works related to localization, clustering and security approaches.It is worth noting that securing wireless sensor networks is a challenging task, as the sensor nodes have limited computational and energy resources [16]. Therefore, it is important to choose efficient security mechanisms with low overhead. In this article, an energy aware clustering mechanism with security measures is proposed.

The proposed ECSCA approach improves network security and efficiency. ECSCA uses fuzzy clustering to intelligently generate clusters based on remaining energy, reachability, and cluster head supremacy. WSN security is enhanced by ECSCA Secured Routing's Elliptic Curve Cryptography (ECC). ECC is known for its mathematical elegance and efficiency over other encryption algorithms. Elliptic curves' unique features encrypt and decrypt data, ensuring safe network communication.

A combination of key characteristics that solve fundamental weaknesses in competing systems distinguishes the proposed idea. In this approach, the Energy Conscious Secured Clustering Algorithm (ECSCA) holistically addresses energy efficiency and security in Wireless Sensor Networks (WSNs), unlike many others. The proposed solution excels due to this unique combination of fuzzy-based non-probabilistic clustering and Elliptic Curve Cryptography (ECC) secured routing:

- Enhanced Energy Efficiency: ECSCA optimises energy usage during cluster formation and data transmission, unlike other ideas that focus simply on clustering or security.
- Improved Reachability: Assesses the degree of reachability of potential cluster leaders, thereby enhancing network connectivity.
- Security: The research solution relies on ECC, which provides strong security without high computational overhead for resource-constrained WSNs.
- Scalability: By deploying small and large WSNs using the proposed technique.
- Static Node Handling: ECSCA handles static nodes, assuring stability, which dynamic node proposals typically ignore.
- Conflict Resolution: ECSCA intelligently uses beacon signals to resolve conflicts between nodes in different clusters.

The article sections are organized in the following manner. Section 2 describes the proposed method, and section 3 discusses the comparison results. Section 4 concludes the research work.

3. Materials and Methods

The materials and methods section should contain sufficient detail so that all procedures can be repeated. It may be divided into headed subsections if several methods are described. The constraints of existing clustering techniques for Wireless Sensor Networks (WSNs) motivate this study. There are two key problems, specifically insufficient energy efficiency and security difficulties. Traditional clustering algorithms frequently use too much energy and do not offer reliable security measures, which restricts their use in real-world applications [17].

The goal of this research is to overcome these obstacles and provide a unique clustering method that allays security and energy inefficiency issues while also improving the overall performance and dependability of WSNs. The novelty of this work lies in developing the Energy Conscious Secured Clustering Algorithm (ECSCA). This approach provides a number of novel aspects that set it apart from currently used clustering algorithms. Secondly, it combines fuzzy logic with non-probabilistic clustering techniques to increase the effectiveness and precision of cluster creation.

It also has an improved security system based on Elliptic Curve Cryptography (ECC), which offers a strong defence against many forms of assaults. A unique strategy for addressing the new problems in secure communication is the use of ECC for secure routing in WSNs. The ECSCA also takes into account the dynamic nature of WSNs by adjusting to various conditions, such as big and small groups of sensor nodes, while making sure that cluster head selection and data transmission are efficient. The proposed scheme consists of

several steps that outline the process. It starts with the selection of a sink threshold (Eth) to determine if a randomly generated value by a node qualifies it as a random cluster head. Nodes are thereafter instructed to choose a random value, and if this amount exceeds Eth, the node is designated as a random cluster head. Otherwise, it remains a standard node.

Table 1. Comparison of related works

Ref. No.	Article Details	Approach	Trade-offs/challenges
[1]	Natraj, N.A.; Bhavani, S. A Certain Investigation on Secure Localization Routing Protocol for WSN. Journal of Theoretical & Applied Information Technology 2017, 95, 22.	SLRP with a 3-phase mechanism 1. Cluster member selection and route formation 2. Localization Procedure 3. Secure Localization scheme	1. It is more complex than other localization algorithms 2. Trade-off between accuracy and energy efficiency is unexplored 3. Overhead of Security Protocol impacts the efficiency
[2]	Le-Ngoc et al. Optimized fuzzy clustering in wireless sensor networks using an improved squirrel search algorithm. Fuzzy Sets and Systems 2021, 438, 26.	Improved squirrel search algorithm (SSA) aimed to improve the energy efficiency and network lifetime of WSNs. 1. Fuzzy Inference System (FIS) 2. Optimization of FIS parameters	1. The focus is on clustering and energy efficiency. 2. Security issues remain unaddressed.
[3]	Hosseinzadeh, M., Yoo, J., Ali, S. et al. A cluster-based trusted routing method using fire hawk optimizer (FHO) in wireless sensor networks (WSNs). Sci Rep 13, 13046 (2023).	1. Cluster-based Trusted Routing Technique to enhance security in WSN through a weighted trust mechanism	1. Focus is on Security mechanisms alone. 2. No analysis on Scalability 3. Less focus on energy efficiency
[5]	Akila, I.S.; Venkatesan, R. An Efficient Energy Harvesting Assisted Clustering Scheme for Wireless Sensor Networks. International Journal on Recent and Innovation Trends in Computing and Communication 2016, 4, 7.	Proposed a 3-phase Energy efficiency approach 1. Data sensing 2. Data forwarding 3. Data Aggregation Leverages energy harvesting and effective clustering to extend the network's lifetime	1. The clustering mechanism and energy efficiency are the main points of interest. 2. Security concerns are still unresolved.
[25]	Boobalan, J., & Malleswaran, M, Secure Cross Layer Energy Supplementing Adhoc On-Demand Multipath Distance Vector (SCES-AOMDV) Routing Protocol for Energy Efficient Design of Wireless Sensor Networks. Adhoc & Sensor Wireless Networks, 54,2022.	1. Secure Cross-layer Energy Supplementing Adhoc on-demand Multipath Distance Vector for enhanced energy efficiency and secured communication	1. The introduction of the OTP mechanism may impact the performance of the system. 2. Focus on secured mechanisms can be improvised
[26]	Banu, S.S., A Secure Multicast Reliability based Authenticated Routing Scheme for Data Integrity in Wireless Sensor Networks. International Journal for Research in Applied Science & Engineering Technology, 8, 2020.	Proposed Reliable Multicast Secure Routing (RMSR) for secured localiztion approach by introducing network model and attack model with the help of PKI.	1. The focus of the clustering mechanism is less. 2. The use of Public key cryptography influences Energy efficiency and performance.
[27]	Nikolidakis, S.A., Kandris, D., Vergados, D.D. and Douligeris, C., 2013. Energy efficient routing in wireless sensor networks through balanced	Proposed a routing protocol called Equalized Cluster Head 7 Election Routing Protocol (ECHERP) with the help of Gaussian Elimination Algorithm	1. The focus is more on clustering and energy efficiency mechanisms. 2. The tradeoff between security and energy efficiency shall be explored.

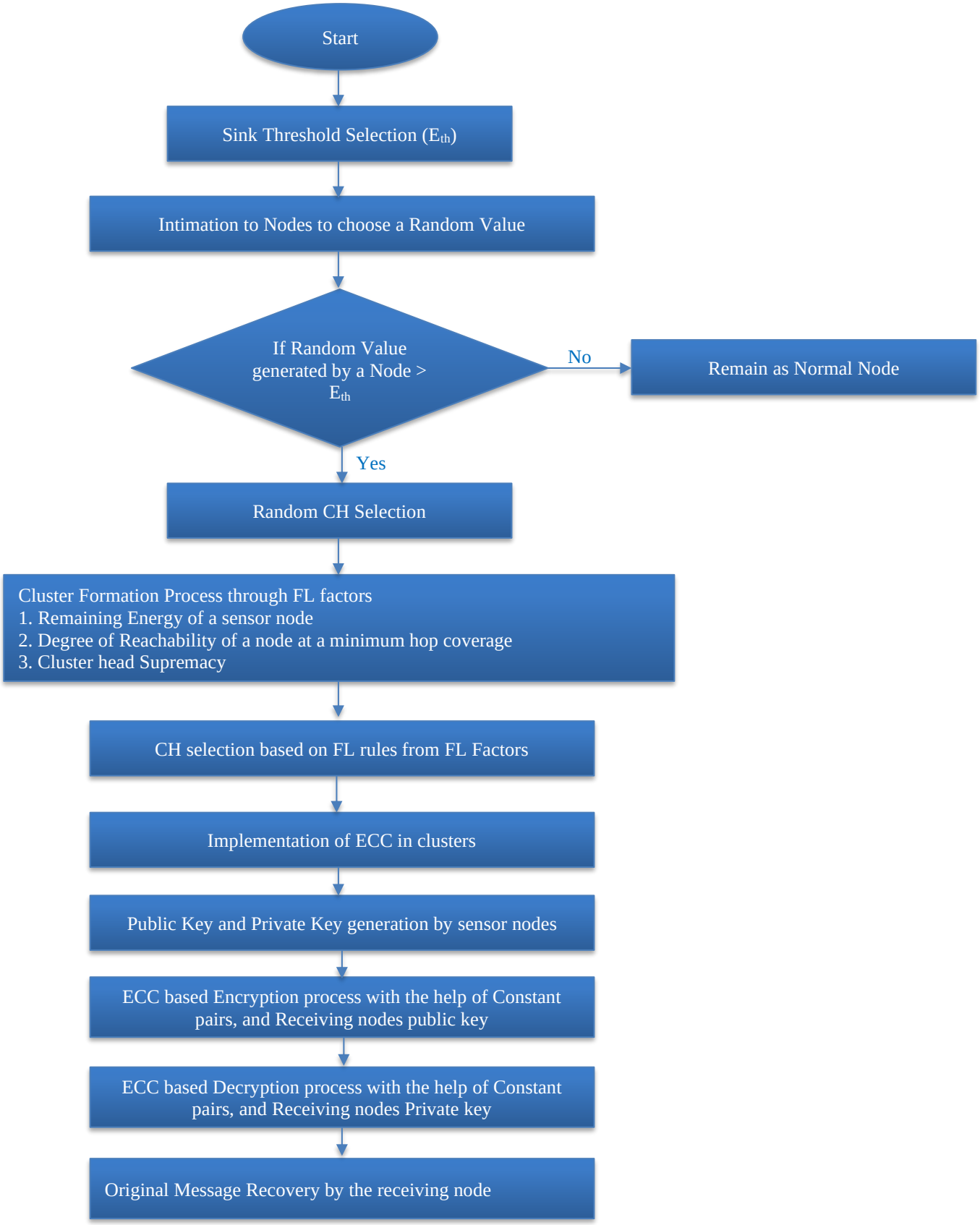

Fig. 2 Flow diagram of the proposed ECSCA algorithm

The cluster creation process begins with fuzzy logic parameters, including the residual energy of sensor nodes, the extent of reachability within a minimal hop range, and the dominance of cluster heads. Cluster heads are selected based on these factors using fuzzy rules. Within the clusters, Elliptic Curve Cryptography (ECC) is implemented, where sensor nodes generate public and private keys. The ECC-based encryption process utilizes constant pairs and the public key of the receiving nodes, while the decryption process employs constant pairs and the private key of the receiving nodes. Finally, the receiving node is able to recover the original message. These steps provide an overview of the proposed scheme, outlining the key processes involved in achieving energy-conscious secured clustering in wireless sensor networks.

Figure 2 represents the flow diagram of the Energy Conscious Secured Clustering Algorithm (ECSCA).The proposed Energy Conscious Secured Clustering Algorithm (ECSCA) is a fuzzy-based non-probabilistic clustering process with an enhanced security mechanism. This method aims to overcome the drawbacks of lack of energy efficiency and security issues in the existing clustering mechanisms. The network propagation model is implemented for big and small sensor node groups using the suggested technique.

Assume unmanned random node deployment. Sensor nodes are static. Node distances are calculated using Euclidean distance. The implementation area is 1000 x 1000 m2, and there are 100 WSN nodes. Initially, source and sink nodes are chosen randomly. The Cluster Head (CH) selection begins after cluster creation. Cluster Heads are responsible for identifying network issues and monitoring cluster members. Cluster members move data packets to their destination. These nodes lack resources and transmission range. As mentioned, the nodes are deployed randomly for cluster formation. The distance of neighboring nodes is computed initially through the Euclidean distance formula.

The sink node creates a threshold value and intimates the sensor nodes to select a random value. When the Random Value generated by the sensor nodes is greater than the Threshold value, then those nodes are considered Random Heads, and these random heads are elected for a certain period of time. Now, the cluster formation should be done. This is done using different factors of fuzzy logic for cluster formation. They are,

1. Remaining Energy of a sensor node
2. Degree of Reachability of a node at a minimum hop coverage
3. Cluster head Supremacy

1. Remaining Energy of a Sensor Node

Nodes with high residual energy are prioritized for cluster head selection. The cluster head is responsible for all node-sink communication; hence, this option is first considered.

2. Degree of Reachability of a node at a minimum hop coverage

This value represents the number of neighbors presents within a minimum hop radius of the putative CH. The neighbor node hop value N_{hop} should lie within the threshold hop valueE_{th}, and it is selected as follows.

$$Neighbour\ N_i = N_{hop} < E_{th}, \quad (1)$$

The degree of reachability identifies the total number of neighbors for the proposed cluster head. From Equation (1), it is expressed as:

$$Degree\ of\ reachability\ = \frac{|N_i|}{Number\ of\ nodes} \quad (2)$$

3. Cluster head (CH) Supremacy

This value determines the effectiveness of the Cluster head. This value determines the consumption of energy by the sensor nodes during the data gathering and data flooding process. The Cluster Head (CH) Supremacy is calculated as follows:

$$Cluster\ head\ Supremacy\ = \frac{\sqrt{\frac{\sum b\varepsilon N_i D^2(a,b)}{N_i}}}{\alpha} \quad (3)$$

Where$D(a,b)$ represents the distance between the nodes a and b. Here, b represents the neighbor node that belongs to $N_i$family. The αrepresents the total area of the network. With the help of Random Cluster Heads, the Main Cluster heads are identified using the parameters mentioned in Table 2. Clustering integrates Table 2 and manages fuzzy rules.

The Random Cluster head sends a beacon signal to the cluster's nodes with its probability value. It may now become a Cluster Head (CH) or member. The cluster head is the appropriate node based on CH probability. Energy left in the sensor node is important. The disagreement between nodes in various clusters may be resolved by tracking the receipt of cluster advertisements via beacon signals from the Random cluster leader. AES is a symmetric-key method used to secure sensitive data like credit card numbers and personal information.

Table 2. Probability of selection as CH

Energy Value	Degree of Reachability	Cluster Head Supremacy	Probability of Selection as CH
High	High	High	High
High	High	Low	Medium
High	Low	Low	Low
High	Low	High	Medium
Medium	Low	Low	High
Medium	High	High	High
Medium	Low	High	High
Medium	Medium	Low	Medium
Low	Medium	High	Medium
Low	High	High	Low

Data is encrypted and decrypted using AES using a fixed-length key (128, 192, or 256-bit). An attacker can interpret the packet flow between the nodes in the network through eavesdropping or by intruding themselves as a node in the network. Effective measures should be taken to protect data from harmful attacks that compromise data security. Security measures should be implemented before the establishment of inter-cluster communication. After the formation of the cluster, the next step is to integrate the security measures in node-to-node communication. This is achieved with the help of Elliptical Curve Cryptography (ECC) methods. It is important to note that the choice of the encryption algorithm and key size will depend on the security requirements of the system and the type of data that is being protected.

3.1. Secure Routing using ECC

Victor Miller and Neal Koblitz initially devised elliptic curve cryptosystems in 1985. Miller and Koblitz thought Elliptical Curve Cryptography (ECC) was mathematically beautiful at the time. Elliptic Curve Cryptography (ECC) is a PKI based on elliptic curve mathematics. ECC uses the properties of an elliptic curve to encrypt and decrypt data rather than the large prime numbers used in traditional methods such as RSA. A smooth elliptic curve is expressed as follows.

$$y^2 = x^3 + ax + b, \tag{4}$$

Where a and b are constants, using specific mathematical formulas, points on the curve can be added and multiplied. These operations can generate a group of points, with a unique point known as the "point at infinity" serving as the identity element. In ECC, the sender encrypts the information with the recipient's public key, an elliptic curve point. The recipient then decrypts the data using their corresponding private key, a number. The difficulty of solving the Elliptic Curve Discrete Logarithm Problem, which is the problem of finding the private key with respect to a given public key, is the foundation of ECC security. One of the primary benefits of ECC over traditional methods such as RSA is that it provides the same level of security while using smaller key sizes. This means that ECC can be used to secure Wireless Sensor Networks (WSNs) with limited resources, as well as IoT devices with limited resources.

Furthermore, ECC is frequently regarded as more secure than traditional methods against quantum computing attacks, as it has been demonstrated that quantum computers would have a more difficult time solving ECDLP than the factorization problem that serves as the foundation for RSA. It is important to note that ECC is a complex topic, and it is strongly advised to consult with experts in the field before implementing it in a system. To improve communication security, an encryption technique based on Elliptic Curve Cryptography (ECC) is used in the context of the suggested approach. ECC has a number of advantages over older encryption systems like RSA. Let us examine and debate the sorts of attacks that ECC aids in resisting, as well as the precise functions it plays in the suggested method.The computational complexity of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) underpins ECC security. This considerably increases the difficulty for attackers in employing brute-force approaches. The mathematical features of ECC add resilience to such assaults. Second, ECC aids in the prevention of key compromise attacks. The encryption procedure in ECC entails safely creating and maintaining keys using elliptic curve features.

This provides a strong defence against assaults aimed at compromising encryption keys. ECC also provides security benefits against quantum computing assaults. It is thought to be more secure in the face of quantum computers than classic encryption techniques such as RSA. Because of the complexity of solving ECDLP, ECC is a viable alternative in the post-quantum computing age. ECC is also effective and suitable for situations with limited resources. Smaller key sizes conserve resources while offering the same degree of security as conventional methods. This element fits in nicely with the paper's discussion of Wireless Sensor Networks' (WSNs') limited resources and energy efficiency.

3.2. ECC based Encryption Process

Assume Node A in a cluster is willing to send a message 'm' to Node B. Now, Node A chooses a positive integer 'i' randomly. With the help of this 'i', a Cipher text is created. The Cipher H_1, consisting of the pair of points, is given by,

$$H_1 = \big(i * G, m + (i * K_B)\big), \tag{5}$$

Where, G is the point on the Elliptic curve whose order is significant value 'i', and node A uses the public key of Node B, which is K_B. If Node B in the cluster is willing to communicate with A, then it should undergo the same process followed by A. B will choose a random positive number. The Cipher text is then created with the help of a pair of points. B utilizes the node's public key with which it wants to interact.

3.3. Decryption Process in ECC

The encrypted message of node A should be decrypted by node B. The decryption procedure involves the multiplication of B with the first point of the pair using the private key. The result is subtracted from the second point.

$$\begin{aligned} m + (i * K_B) \; - \; & P_B(i * G) \\ & = \; m + i * (P_{B*}G) - P_B(i * G) \; = \; m \end{aligned} \tag{6}$$

In equation (6), node A has hidden the message 'm' using the public key of 'i'. Now, even if the public key.

4. Results and Discussion

The proposed method ECSCA was simulated using the network simulator tool (ns-3) [25]. The simulation settings are given in Table 3.

Table 3. Simulation parameters

Parameters used	Values
Total nodes	100
Size of Area	1000 x 1000 m^2
MAC	LR-WPAN
Time taken in simulation	100 Sec
Size (Packet)	512 bytes
Motion Model	Random Walk Model
Protocol	ECSCA

4.1. Node Location Accuracy

The amount of exact topographical positions of nodes that are typical to the overall number of predicted locations. The simulation results were compared with the existing methods SLRP [1], RMSR [26] and ECHRP [27] and ECSCA proved to be better in terms of Node location accuracy. The node location accuracy of the proposed method proves to be better than the existing method by 14.34%. Figure 3 shows the comparison results of the Node Accuracy encrypted message.

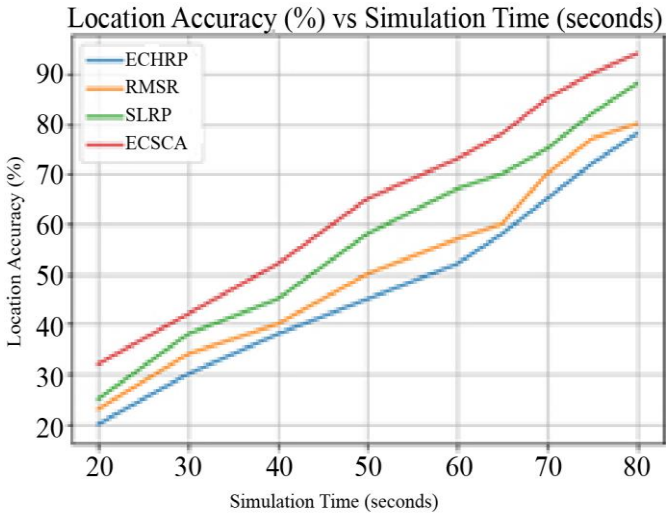

Fig. 3 Location accuracy vs. Simulation time

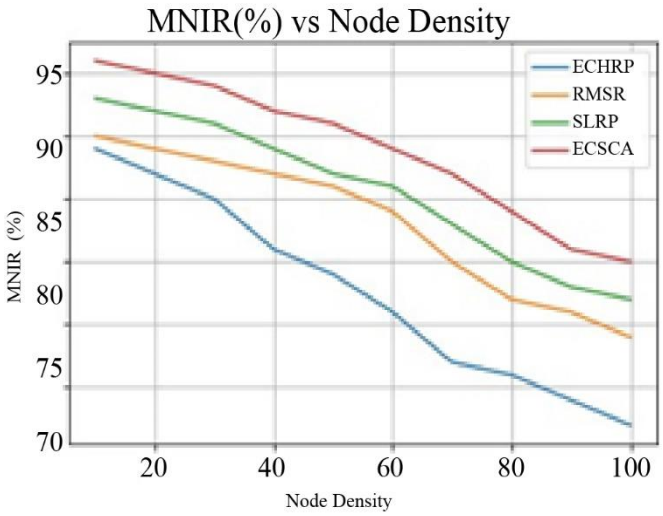

Fig. 4 Performance analysis for energy efficiency (%)

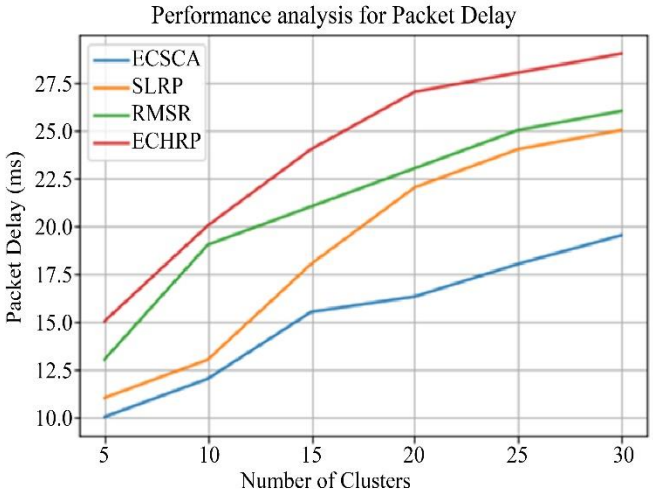

Fig. 5 Performance analysis for packet delay

4.2. Energy Efficiency

The amount of energy the sensor nodes use over the simulation time. The energy consumed by sensor nodes in the ECSCA scheme proved to be better than the existing methods like SLRP [1], RMSR [26], and ECHRP [27] scheme by 2.352%. In the existing scheme, the concentration was more on location integrity and security mechanisms than energy efficiency. Figure 4 represents the comparison results of ECSCA with the existing methods for Energy efficiency.

4.3. Packet Transmission Delay

This represents the transfer of packets from the origin to the destination node over a span of time. The Members of the cluster and their packet transfer delay are compared with the existing methods. In Figure 5, the ECSCA shows a slight improvement of 3.02% due to the proposed fast cluster formation process compared with the existing method. The proposed research also uses ECC, which has fewer overheads compared to the other cryptography methods.

4.4. Packet Rate Delivered

The ratio of packets transferred with packets successfully obtained at the receiver end over the route from the source is referred to as the packet rate delivered. The number of preceding hops is also considered while the ratio is calculated. In Figure 6, the proposed research proves to be better by 2.92 % in terms of number of packets delivered over a period of time.

4.5. Ratio of Malignant Node Detection

The statistical ratio of malicious nodes to cluster members is known as the Malignant Node Identification Ratio (MNIR). From Figure 7, it is observed that the Malicious node identification in the presence of the highest node density is better by 3.90%in the ECSCA method than in the SLRP method and the other methods. The overall goal of this study is to resolve security and energy efficiency problems with current counselling techniques for WSNs.

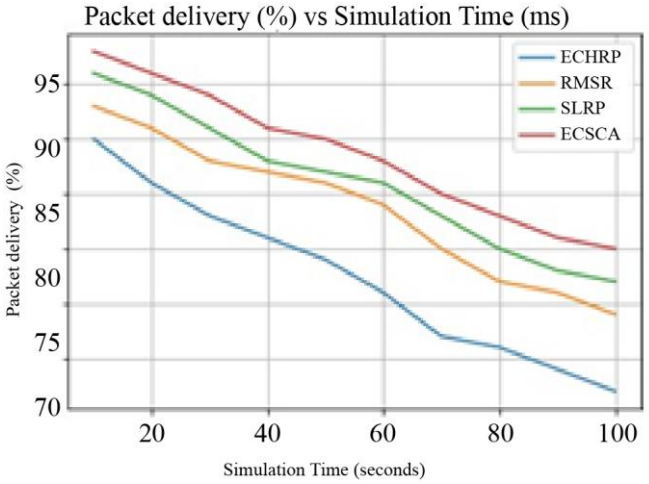

Fig. 6 Performance analysis for packet delivery

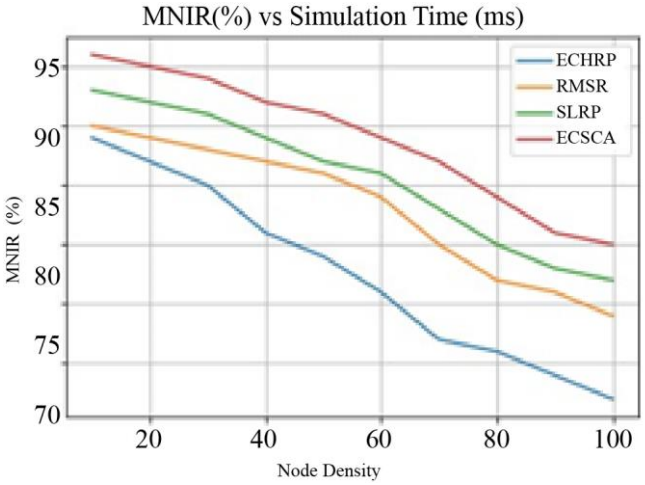

Fig. 7 Performance comparison of MNI ratio

The innovation comes in the creation of the ECSCA, which blends non-probabilistic clustering, fuzzy logic, and ECC-based secure routing to deliver enhanced performance, robust security, and energy efficiency. This research provides a significant addition to the field of WSNs by resolving these issues and providing novel characteristics, as well as opening up new directions for future study and development in this area.

5. Conclusion

The Energy Consumption by sensor nodes during the data gathering process is a major concern in wireless sensor networks. Securing the sensor network from malignant nodes should also be the focus. Balancing these two constraints, an Energy Conscious Secured Clustering Algorithm (ECSCA) method is proposed to obtain an energy efficient secured network. Energy Conscious clustering process is done using fuzzy based factors, and the integration of security measures is carried out through Elliptic Curve Cryptography.

Different performance metrics were analyzed and compared between the existing and the proposed method. Simulated results depict that the proposed ECSCA outperformed the Secured Localization Routing Protocol (SLRP) and other existing methods like RMSR [26] and ECHRP [27] in various performance metrics. The Node location accuracy was identified to be 14.34% better than the existing methods. In terms of Energy Efficiency, the ECSCA is found to be 2.352% better than the existing methods. In terms of Packet transfer delay, the proposed ECSCA showed 3.02% better than the existing method.

The packets delivered by the proposed ECSCA method are found to be better by 3.90% than the existing methods. A balanced output is obtained, which satisfies both energy efficient clustering and secured node-to-node communication. ECSCA fills a major research need by presenting a holistic solution that prioritises energy efficiency and security, unlike solutions that prioritise one over the other. A balanced output is obtained, satisfying both energy-efficient clustering and secured node-to-node communication.

ECSCA fills a major research need by presenting a holistic solution that prioritizes energy efficiency and security, unlike solutions that prioritize one over the other. One of the aspects that are not considered in this work is the scalability of the proposed ECSCA (Energy Conscious Secured Clustering Algorithm), which plays a major role in the clustering as well as the data gathering process. Hence, focusing on the enhancement of clustering and efficient data-gathering processes embedded with ECSCA will be another exciting area of future work.

References

[1] N.A. Natraj, and S. Bhavani, "A Certain Investigation on Secure Localization Routing Protocol for WSN," *Journal of Theoretical & Applied Information Technology*, vol. 95, no. 22, pp. 6022-6031, 2017. [Google Scholar] [Publisher Link]

[2] Kim Khanh Le-Ngo et al., "Optimized Fuzzy Clustering In Wireless Sensor Networks Using Improved Squirrel Search Algorithm," *Fuzzy Sets and Systems*, vol. 438, pp. 121-147, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mehdi Hosseinzadeh et al., "A Cluster-Based Trusted Routing Method Using Fire Hawk Optimizer (FHO) in Wireless Sensor Networks (WSNs)," *Scientific Reports*, vol. 13, no. 1, pp. 1-20, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Bhisham Sharma, Yogesh kumar, and Vandana Ladha, "Design and Develop ECC for Wireless Sensor Network," *International Journal of Computer Applications*, vol. 39, no. 16, pp. 1-7, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[5] I.S. Akila, and R. Venkatesan, "An Efficient Energy Harvesting Assisted Clustering Scheme for Wireless Sensor Networks," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 4, no. 4, pp. 548-558, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[6] P. Thangaraju, and S. Kanjana, "A Secure Energy Efficient and Aware Protocol for WSN," *International Science Press*, vol. 9, no. 26, pp. 357-362, 2016. [Publisher Link]

[7] Junqi Duan et al., "TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[8] I.S. Akila, S.V. Manisekaran, and R. Venkatesan, *Modern Clustering Techniques in Wireless Sensor Networks*, Wireless Sensor Networks - Insights and Innovations, IntechOpen, London, United Kingdom, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Pooja Gulganwa, and Saurabh Jain, "EES - WCA: Energy Efficient and Secure Weighted Clustering for WSN Using Machine Learning Approach," *International Journal of Information Technology*, vol. 14, pp. 135-144, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Reenkamal Kaur Gill, Priya Chawla, and Monika Sachdeva, "Study of LEACH Routing Protocol for Wireless Sensor Networks," *International Conference on Communication, Computing & Systems (ICCCS–2014)*, pp. 196-198, 2014. [Google Scholar] [Publisher Link]

[11] V. Vijayalakshmi, and T.G. Palanivelu, "Secure Localization Using Elliptic Curve Cryptography In Wireless Sensor Networks," *International Journal of Computer Science and Network Security*, vol. 8, no. 6, pp. 255-261, 2008. [Google Scholar] [Publisher Link]

[12] Chada Sampath Reddy, and G. Narsimha, "Secure Optimized Routing and Data Transmission in Wireless Sensor Networks with Elliptic Curve Cryptography," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 4, pp. 279-291, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Celso Moraes, and Dongsoo Har, "Charging Distributed Sensor Nodes Exploiting Clustering and Energy Trading," *IEEE Sensors Journal*, vol. 17, no. 2, pp. 546-555, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[14] Hong Fu, Xiaoming Wang, and Yingshu Li, "Adaptive Energy and Location Aware Routing in Wireless Sensor Network," *Wireless Algorithms, Systems, and Applications: 5th International Conference*, Beijing, China, pp. 105-109, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[15] Kashif Naseer Qureshi et al., "Optimized Cluster-Based Dynamic Energy-Aware Routing Protocol For Wireless Sensor Networks In Agriculture Precisión," *Journal of Sensors*, vol. 2020, no. 1, pp. 1-19, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Amine Rais, Khalid Bouragba, and Mohammed Ouzzif, "Routing and Clustering of Sensor Nodes in the Honeycomb Architecture," *Journal of Computer Networks and Communications*, vol. 2019, no. 1, pp. 1-12, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Hamid Mahboubi et al., "Maximum Lifetime Strategy for Target Monitoring with Controlled Node Mobility in Sensor Networks with Obstacles," *IEEE Transactions on Automatic Control*, vol. 61, pp. 3493-3508, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[18] CS. Firdozali, and T. Nagamalar, "Energy Aware Mobile Sink Based RPL Routing Protocol for Wireless Sensor Networks," *International Journal of Latest Technology in Engineering*, vol. 5, no. 4, pp. 74-78, 2016. [Google Scholar] [Publisher Link]

[19] Amjad Mehmood et al., "Improvement of the Wireless Sensor Network Lifetime Using LEACH with Vice-Cluster Head," *Adhoc & Sensor Wireless Networks*, vol. 28, no. 1-2, pp. 1-23, 2015. [Google Scholar] [Publisher Link]

[20] Amjad Mehmood et al., "Energy-Efficient Multi-Level and Distance-Aware Clustering Mechanism for WSNs," *International Journal of Communication Systems*, vol. 28, no. 5, pp. 972-989, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[21] Meble Varghese, and M. Victor Jose, "Securing Cloud from Attacks: Machine Learning Based Intrusion Detection in Cloud Sensor Networks," *Adhoc & Sensor Wireless Networks*, vol. 50, no. 1-4, 2021. [Google Scholar] [Publisher Link]

[22] Miguel Garcia et al., "Saving Energy and Improving Communications using Cooperative Group-Based Wireless Sensor Networks," *Telecommunication Systems*, vol. 52, pp. 2489-2502, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[23] Raquel Lacuesta et al., "A Secure Protocol For Spontaneous Wireless Ad Hoc Networks Creation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 629-641, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[24] Jaime Lloret et al., "A Cluster-Based Architecture to Structure The Topology of Parallel Wireless Sensor Networks," *Sensors*, vol. 9, no. 12, pp. 10513-10544, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[25] J. Boobalan, and M. Malleswaran, "Secure Cross Layer Energy Supplementing Adhoc On-Demand Multipath Distance Vector (SCES-AOMDV) Routing Protocol for Energy Efficient Design of Wireless Sensor Networks," *Adhoc & Sensor Wireless Networks*, vol. 54, no. 3-4, pp. 219-248, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[26] S. Saira Banu, "A Secure Multicast Reliability based Authenticated Routing Scheme for Data Integrity in Wireless Sensor Networks," *International Journal for Research in Applied Science & Engineering Technology*, vol. 8, no. 4, pp. 1558-1563, 2020. [Google Scholar] [Publisher Link]

[27] Stefanos A. Nikolidakis et al., "Energy Efficient Routing In Wireless Sensor Networks Through Balanced Clustering," *Algorithms*, vol. 6, no. 1, pp. 29-42, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[28] NSNAM Files, Source Forge. [Online]. Available: https://sourceforge.net/projects/nsnam/files/allinone/ns-allinone-2.34/ns-allinone-2.34.tar.gz/download.