International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 18s, 2025
https://theaspd.com/index.php

Fuzzy-DEEC Protocol And FPA-Optimized ECC For Secure And Energy-Efficient Wireless Sensor Network

Vikas Kumar Mishra[1], **Dr. Rajesh Kumar Nagar**[2]
[1]Research Scholar, SAGE University, Indore, mishra.vikas95@gmail.com
[2]Associate Professor, SAGE University, Indore

Abstract: *The current requirement in Internet of Things (IoT) applications is the use of Wireless Sensor Networks (WSN) which must be both energy-efficient and have secure data transmission. In this paper, a new hybrid system is presented, as well as Distributed Energy-Efficient Clustering (DEEC) protocol was set in conjunction with Elliptic Curve Cryptography (ECC) and Fuzzy Logic or what is called Fuzzy-DEEC Protocol. The protocol that is proposed focuses on improving the performance of WSN by intelligent cluster head selection and secure communications. ECC parameters are also optimized which minimizes computational demand and enhances performance by the usage of Flower Pollination Algorithm (FPA). As shown by our simulation, Fuzzy-DEEC Protocol is better than standard DEEC in several ways, regarding energy consumption, network lifetime, throughput, packet drop rate. In particular, the protocol attains 30-50% longer network life, 15-25% lower energy costs, 25-40% higher throughput, and 35-45% lower packet drop-rate. These benefits are attributed to the fact that selection of cluster heads has been optimised, energy aware routing and secure data transmission is implemented. The effectiveness of this protocol is confirmed with complete performance measures including quantity of active nodes surviving in time, network bandwidth, energy usage and packet drop percentage. This paper prepares the ground to more improved WSN safe and sustainable architecture and thus it is suited to WSN implementation in industrial monitoring, smart agriculture and remote sensing.*
Keywords: *Wireless Sensor Networks (WSNs), Fuzzy, FPA, DEEC Protocol, ECC Cryptography, etc.*

I. INTRODUCTION

Wireless Sensor Network (WSN) is a crucial part of contemporary Internet of Things (IoT) applications and can provide a wide range of applications, including environmental monitoring, medical, industrial automated systems, smart cities, and surveillance in the military. WSNs are systems composed of spatially-distributed sensor nodes gathering and relaying data to an access point (central-base station-BS) [1]. The networks are essential in gathering real time important information about the surrounding environment including temperature, humidity, motion, lighting as well as other physical measures. Nevertheless, there are a number of inherent challenges to WSNs that impair the successful implementation of WSNs in some applications as well as their sustainability in the long run. Two main issues among them include energy efficiency [2] and safe data passage. The availability of sensor nodes in WSNs is of the key consideration, since the nodes are always battery-powered and deployed in isolation or hostile regions, efficient use of available energy resources as well as protection against possible attacks are highly essential to the success of WSNs.

Problem Definition: Two primary challenges must be addressed to optimize the performance of WSNs:

- **Energy Efficiency:** WSNs have to work under the limitation of sensor node battery capacity. Sensing, processing and the transmission of data are all continuously taking place, which can easily drain the energy bank of the sensor nodes failing the whole network early on. Thus, it is important to properly control the consumption of energy in order to prolong the working life of the network [4]. The classic strategies can lead to the unbalanced distribution of energy throughout the network, as some of its nodes spend much more energy than others, which makes them fail in the early stages and decreases the level of network performance.
- **Security:** The WSNs are normally installed in an environment where they are prone to external attack such as eavesdropping, unauthorised access to data and alteration of data. The information being passed between the systems are sometimes a very sensitive one (e.g. environmental conditions, health data, or military intelligence) and it is utmost important to secure this information against the unauthorized access. Sensor nodes are by their nature resource constrained, and using conventional

cryptoperative protocols such as RSA or AES [5] may easily become prohibitively expensive in both computational and energy costs, which is not acceptable in these environments.

These two issues energy efficiency and security are perceived to be separate and it is perceived that to secure data there is need to increase additional computational overheads which in turn consumes more energy. Therefore, the ability to come up with a solution that can effectively solve both the challenges concurrently is a potential research question in the development of WSNs.

Motivation: The inspiration of this study comes through the increasing demands of more resilient, secure, and energy-efficient WSNs in IoT applications. As sensor networks come to be installed in more and more crucial applications, including healthcare, environmental sensors, and smart cities, there is a pressing necessity to make sure that not only will the networks be reliable and efficient but also secure against possible attacks. Specifically, the security and longevity of the sensor nodes is essential in the case of a remote medical monitoring system, industrial, and environmental data gathering, etc. The existing solutions usually tend to either deal with maximization of the energy efficiency or bolster the security, with very little solutions trying to do the two at the same time. Closer combinations between lightweight cryptography techniques and energy efficient [6] clustering protocols could also represent a tradeoff ideal situation that preserves network performance still promises the network integrity and security of the information. In large-scale WSNs, in particular, this strategy is of particular importance because resource maintenance is essential to any long-term sustainability.

Contribution: In the present paper, we suggest a new hybrid scheme to combine Distributed Energy-Efficient Clustering (DEEC) Protocol with Elliptic Curve Cryptography (ECC) and Fuzzy Logic. Such combined solution, known as the Fuzzy-DEEC Protocol is expected to optimize not only energy efficiency but also data security in WSNs. The main points of this work are the following:

- **Energy-Efficient Clustering with Fuzzy Logic:** Our contributions over the DEEC protocol will be in the addition of Fuzzy Logic in order to provide intelligent cluster head (CH) selection. Conventional DEEC is based on clustering by energy, and it can further be enhanced through the utilization of multi-parameter including, the energy level, the centrality of nodes, the density of node and distance to the base station (BS). A more dynamic and smart decision-making process is possible with the fuzzy logic system in the selection of the cluster heads thus enhancing the overall performance of the network and energy consumption.
- **Lightweight Cryptography with ECC:** To handle the security issue in WSN, we combine Elliptic Curve Cryptography (ECC) to make it secure to transmit data. ECC is a low-weight cryptography process which provides high level of security with lesser key sizes than conventional cryptography processes, e.g. RSA. It renders ECC to be a cost-effective solution to the resource-limited sensor node since it lessens the computation and energy cost overheads in encrypting and decrypting data.
- **Optimizing ECC Parameters using FPA:** The ECC implementation is also optimized by fine tuning the cryptographic parameters that we achieve using Flower Pollination Algorithm (FPA). Optimization of ECC parameters will allow them to save energy because the minimal work will be done on the sensor nodes to achieve high security.

Comprehensive Performance Evaluation: Our simulations are performed thoroughly in order to consider the effectiveness of the suggested Fuzzy-DEEC Protocol in comparison with the traditional DEEC protocol. The performance shows that a substantial increase in a wide range of performance metrics include:

- **Network Lifetime:** Fuzzy-DEEC Protocol has been able to increase 30% to 50 % the network lifetime due to optimization of cluster head selection and energy-aware routing.
- **Energy Consumption:** It is due to optimized clustering and parameter tuning of ECC that our protocol decreases the amount of energy consumed by 15-25 %.
- **Throughput:** An experience of improvement in throughput of network of around 25-40% that result in better efficiency in transmission of data.
- **Packet Drop Rate:** The protocol reduces packet drop rates by 35-45%, ensuring more reliable communication.

Realistic Simulation and Performance Metrics: The simulator includes the energy usage, data transmission in secure mode and network dependability. We monitor important performance parameters like number of alive nodes with the passage of time, number of cluster heads per round, throughput rate of the network, energy usage and packet drop ratio. The metrics help to get an overall picture of the protocol operations under the real-life conditions.

This paper offers an all-inclusive response to both issues of energy efficiency and WSNs security. It is proved that Fuzzy-DEEC Protocol that has integrated intelligent clustering, ECC-based encryption and optimization functions, can dramatically improve the performance, security and sustainability of wireless sensor networks. Such a strategy is promising in many IoT-based solutions, such as industrial monitoring, smart agriculture, remote sensing, and healthcare; however, in all of them, energy efficiency and data security are essential. The findings open door to leading the design of secure, energy-efficient and scalable WSN architectures.

II. LITERATURE REVIEW

2.1. Introduction to Wireless Sensor Networks (WSNs)

Wireless Sensor Networks (WSNs) have got autonomous sensor nodes temporally distributed over space and they monitor different environmental factors like temperature, pressure, movement and humidity. The potential use of self-configuring networks and infrastructure-free nature of these networks have wide application in a variety of applications; smart agriculture, healthcare monitoring, industrial automation, military surveillance, etc. [7] Energy efficiency is one of the key issues of WSNs because sensor nodes normally use battery power but may be limited in their resources. Since the radio communication is the most energy consuming process in WSNs [8] energy consumption optimization is an important concern to increase the operational life of the network. The key issue to deal with will be to minimize energy consumption at the expense of quality of service, reliability as well as data throughput.

2.2. Network Architectures: Heterogeneous vs. Homogeneous WSNs

WSNs are categorized into two primary types: homogeneous and heterogeneous networks, which differ in terms of node capabilities and energy management strategies.

- **Homogeneous Networks:** In homogeneous networks [9], the sensor nodes share the same energy, processing capabilities and memory. The difference is that these networks are simple to configure and operate since they are uniform. They are however afflicted with unequal treatment of energy use since all nodes are equally engaged in data computation and transfer hence premature death of the nodes becomes a common occurrence.
- **Heterogeneous Networks:** In contrast with homogeneous networks, in heterogenous networks there are nodes that vary in energy and calculation ability. In such networks the nodes that possess more energy and are relatively more advanced can perform more critical operations, e.g. cluster head (CH) or data aggregator of other nodes. This feature enables network efficiency, life span and more efficient energy use [10]. The networks are very beneficial especially in large scale deployment where management and optimization of resources and energy are relevant.

2.3. Energy-Efficient Routing Protocols

A number of energy-efficient routing protocols have been proposed to improve the performance of WSNs and each protocol will focus on various issues of energy management. Such protocols can be reduced to cluster-based protocols and chain based/threshold-driven protocols with each having differing benefits and drawbacks.

2.3.1. Cluster-Based Protocols

- **LEACH (Low-Energy Adaptive Clustering Hierarchy):** One of the first distributed clustering protocols is LEACH [11] in which the heads are probabilistically selected by the nodes themselves. LEACH makes sure that there is an even energy load distribution by rotating the cluster head responsibility among the nodes, so the energy efficiency of the network increases to a great extent. Nevertheless, LEACH assumes that similar energy levels can be found in all nodes, which is why it is not

adapted to heterogeneous networks as well. Also LEACH disregards the distance between the nodes and the base station, and this can lead to inefficient use of energy in larger networks.

- **LEACH-C (LEACH Centralized):** Leach-C [12] enhances LEACH where the base station (BS) is allocated the responsibility of selecting the cluster head. The BS makes decisions on the selection of the best cluster heads according to the global network status, which enhances energy. Nevertheless, the fact that this strategy imposes extra computational load since the cluster head selection process should be maintained ongoing by the BS at all times may prove to be a problem in somewhat large scale networks since selection process may create a bottleneck.
- **SEP (Stable Election Protocol):** SEP [13] was devised on heterogeneous networks and sets the probability of cluster selection to be weighted. The nodes that consume more energy are advanced nodes and therefore have higher chances of making it as cluster parts thereby balancing energy consumption and enhancing network lifetime. Nevertheless, SEP faces energy imbalances due to energy drainage of nodes with higher duties, thus, resulting to inefficient use of energy.
- **DEEC (Distributed Energy-Efficient Clustering) and DDEEC (Developed DEEC):** DEEC [14] dynamically selects the cluster heads considering remaining energies of the nodes that will allow more efficient distribution of the energy. This further is extended under the DDEEC protocol [15] Although these protocols enhance energy distribution they fail to factor in inter-node distances to base station and thus fail to provide an optimal route in big WSN networks.

2.3.2. Chain-Based and Threshold-Driven Protocols

- **PEGASIS (Power-Efficient GAthering in Sensor Information Systems):** PEGASIS [12] does not go through the cluster mechanism, but in its place, a chain of nodes is formed over which the data will be transmitted. In such system, it is only the leader node in the chain that is able to transmit data to the base station which greatly minimizes overheads in the process of communication and saves on energy. PEGASIS however, adds large latency and cannot be used on dynamic networks whose topology varies quickly.
- **TEEN (Threshold-Sensitive Energy-Efficient Sensor Network):** Teen protocol [16] employs both hard and soft thresholds to limit the transmission of data when sensor nodes send information and thus eliminating needless communication as well as saving energy. TEEN is extremely energy-efficient, but it is inappropriate to use it in applications where a periodical reporting is needed since data has to be transmitted only when the threshold conditions are reached that in turn may not always happen.
- **APTEEN (Adaptive Periodic TEEN):** APTEEN [17] is more flexible than TEEN since it allows periodic data transmission as well as event-driven data transmission. The overhead caused by the elaborate threshold mechanics of the protocol however decreases scalability especially on large networks.

2.4. Emerging Trends and Future Directions

Current studies on WSN involve embedding hybrid protocols, dynamic clustering, and machine learning tools to maximize on energy efficiency. Hybrid protocols introduce the power of several existing protocols and serve more flexible and effective networks. Also, with the rise in implementation of WSNs in IoT applications, security issues have led to introduction of lightweight cryptography methods, including Elliptic Curve Cryptography (ECC) which offers a high degree of security but with the minimal computational expense. Energy efficiency and security are becoming the topics of interest as more and more attention should be paid to the aspects of secure communication in resource-constrained practices. The work on distance based optimization techniques keeping in consideration the node proximity to base station and the energy-aware clustering such as DEEC[18] and DDEEC in future WSNs energy-efficient protocols is to be concentrated on. Furthermore, lightweight encryption algorithm, e.g., ECC must be included so that the communication is safe but energy resources are not wasted. Dynamic adaptation techniques which may involve the use of machine learning to make real-time changes will also enhance the network efficiency and its performance.

Although the current routing protocols of WSN such as LEACH, SEP and DEEC have gone a long way in order to enhance energy efficiency, they still exist various challenges including energy balancing, distance optimisation and introduction of security measures. In future, future research must exercise

interest in the hybrid solutions [19] that will implement the powers of energy-efficient routing, lightweight cryptography, and adaptive clustering techniques to maximize the network life and data secrecy. These developments are critical to the creation of long-lived, secure and scalable WSNs in many IoT in different applications where energy consumptions and security are the most crucial aspects.

III. PROPOSED METHODOLOGY

3.1. Energy Consumption Model

In wireless communication networks energy consumption is an important factor in order to achieve efficient operations and long lifespan of devices. Energy will be defined to transmit and to receive data with the help of the first-order radio model. The components of energy consumption are explained in details below:

3.1.1. Transmission Energy (E_{TX})

The energy consumed throughout the transmission of the data is influenced by the size of the packet being sent out, the distance between each node, and also the environmental circumstances (e.g. free space or multi-path fading). The overall transmission energy exists:

$$E_{TX}(k,d) = \begin{cases} k.E_{elec} + k.\epsilon_{f_s}.d^2 & \text{if } d<d_0 \\ k.E_{elec} + k.\epsilon_{m_p}.d^4 & \text{if } d\geq d_0 \end{cases}$$

(1)

Where:

- k = packet size (bits)
- d = distance between the sender and receiver (meters)
- E_{elec} = energy consumed by the electronics (50 nJ/bit)
- ϵ_{f_s} = energy consumed per unit distance for free space (10 pJ/bit/m²)
- ϵ_{mp} = energy consumed per unit distance for multipath fading (0.0013 pJ/bit/m^4)
- d_0 = threshold distance, where the behaviour changes from free space to multipath fading.
- The first equation applies when the distance between nodes is below a certain threshold d_0, where free space propagation dominates, while the second equation governs energy consumption when the distance is larger than d_0 , and multipath fading becomes significant.

3.1.2. Reception Energy (E_{RX})

The amount of energy used in the reception of data will mostly depend on the size of the packet: the amount of energy that the receiving electronics needs:

$$E_{RX}(k) = k.E_{elec}$$

(2)

Where:

- k = packet size (bits)
- E_{elec} = energy consumed by the electronics during reception (50 nJ/bit).

3.1.3. Data Aggregation Energy (E_{DA})

Data aggregation is a process in sensor network where several data packets of various sensors are merged and sent to a central or base station (BS). Energy needed to aggregate data is as follows:

$$E_{DA} = k.E_{agg}$$

(3)

Where:

- k = number of bits in the data packet
- E_{agg} = energy consumed for aggregating data (5 nJ/bit/message).

Aggregation of the data also involves the reduction of the size of data to be transmitted thereby resulting into a number of savings in the amount of energy that would have been consumed. The simulation to be done incorporates various elements in order to improve power consumption and security in Wireless Sensor Networks (WSNs). In particular Fuzzy-DEEC Protocol and Flower Pollination Algorithm (FPA) -

optimized Elliptic Curve Cryptography (ECC) [20] are jointly used in smart cluster head (CH) election and energy-efficient data delivery. The theoretical basis of such methods is described beneath and the involved mathematical formulas are given.

3.2. Fuzzy-DEEC Protocol for Cluster Head Election

The Fuzzy-DEEC protocol is an attempt to enhance the normal DEEC (Distributed Energy-efficient Clustering) [21] towards including Fuzzy Logic in the election of cluster heads. This hybrid algorithm integrates various parameters in order to identify the probability on each node of becoming a cluster head depending on its energy level, centrality, density and distance to the base station (BS).

3.2.1. Fuzzy Logic System

A Fuzzy Inference System (FIS) [22] is used to evaluate the probability of each node becoming a cluster head. The inputs to the fuzzy system are:

- Energy: The residual energy of the node.
- Centrality: The centrality of the node, which indicates its importance within the network.
- Density: The number of neighbouring nodes within a specified radius.
- Distance to Base Station: The physical distance from the node to the BS.

The function of the fuzzy system is that the output is a Cluster Head Probability (CH Probability) value which specifies the probability that a node will be chosen as cluster head. The membership functions Low, Medium and High are used in the fuzzy system in every input variable. The fuzzy rules are intentioned to consider the fact that the nodes that have great energy, centrality, and density, located near the BS have increased chances to become a cluster head.

3.2.2. Mathematical Representation of Fuzzy Logic

For each input variable X (where$X \in \{\text{Energy, Centrality, Density, Distance}_{BS}\}$, the fuzzy membership function is represented as follows:

$$\text{Low: } \mu_l(x) = \frac{1}{1 + \exp\left(\alpha(x - \beta)\right.} \tag{4}$$

$$\text{Medium: } \mu_M(x) \ = \text{Trapezoidal Membership Function (trimf)} \tag{5}$$

$$\text{High: } \mu_H(x) = 1 - \mu_L(x) \tag{6}$$

Here $\mu_L(x)$, $\mu_M(x)$, and $\mu_H(x)$ represent the membership values of the input variables for Low, Medium, and High, respectively. The output $CH_{Probability}$ is determined using the fuzzy rules, such as:

$$CH_{Probability} = \sum_{i=1}^{N} w_i \times \mu_i \tag{7}$$

Where w_i is the weight assigned to each input variable (in this case, the weighted average of energy, centrality, density, and distance to BS) and μ_i is the membership value corresponding to the rule output.

3.3. FPA-Optimized ECC for Secure Data Transmission

The second important element of the suggested approach is that Elliptic Curve Cryptography (ECC) is used to cryptographically transfer messages between nodes. ECC is a low-weight cryptographic solution, which fits into resource-scarce operating system and environments such as WSNs. The ECC parameters, especially, the scalar multiplication operation, which is computationally costly, are optimized using the Flower Pollination Algorithm (FPA).

3.3.1. Elliptic Curve Cryptography (ECC)

ECC operates on elliptic curves defined over finite fields. The elliptic curve is typically expressed in the form:

$$y^2 = x^3 + ax + b|p| \tag{8}$$

Where a and b are constants defining the curve, and p is a large prime number defining the finite field. The point multiplication operation in ECC is central to its security and involves calculating:

$$k.P = (x_3, y_3)$$

(9)

Where $P = (x, y)$ is a point on the elliptic curve and k is a scalar (private key). The multiplication is performed through repeated addition of points on the curve, and this process forms the basis of ECC's security.

3.3.2. Optimized ECC Point Multiplication using FPA

The Flower Pollination Algorithm (FPA) is used to optimize the scalar k in the ECC point multiplication process. The FPA aims to find the best scalar value that minimizes the computational cost associated with point multiplication. This is achieved by adjusting the value of k over multiple iterations.

There are two types of pollination in FPA, the local and global pollination. The local pollination is seeded on the behaviour of pollinators of flower, and the global pollination is induced by a Levy flight. The optimisation in tabula rasa is done mathematically as:

$$k^{new} = k + \delta \times (k^{best} - k)$$

(10)

Where k^{best} is the best solution found so far, δ is a random step size, and k is the current scalar. The global pollination involves Levy flight, which is modeled as:

$$L = \lambda \times \left(\frac{1}{\alpha}\right)^{\frac{1}{\lambda}}$$

(11)

Where λ is the Levy flight parameter, and α is a random step size.

3.3.3. Optimized ECC Point Multiplication Equation

The point multiplication with the optimized scalar k_{opt} is given by:

$$k_{opt}.P = (x_{opt}, y_{opt})$$

(12)

The efficiency of the operation is improved by using the optimized scalar k_{opt}, which reduces the computational cost compared to standard ECC point multiplication.

3.4. Combined Method for Secure and Efficient WSNs

The hybrid technique increases WSN energy consumption and data protection. Fuzzy-DEEC protocol allows smart selection of cluster heads in an energy, centrality, density and distance to the base station. Simultaneously, the low computational overhead associated with the secure data transmission by the FPA-optimized ECC provides the overall improvement in network performance.

3.4.1. Energy Consumption Calculation for Transmission

The energy consumption for data transmission is calculated as:

$$E_{tx} = E_{TX} \times L + E_{FS} \times L \times d^2 \quad (\text{for short} - \text{range transmission})$$

(13)

$$E_{tx} = E_{TX} \times L + E_{MP} \times L \times d^4 \quad (\text{for short} - \text{range transmission})$$

(14)

Where:

- E_{TX} is the energy per bit for transmission,
- L is the packet length in bits,
- d is the distance between nodes.

3.4.2. Security Performance

The security performance is evaluated by calculating the total time for encryption and decryption using ECC. The average time for encryption T_{enc} and decryption T_{dec} is:

$$T_{enc} = \sum_{i=1}^{N} T_{enc_i} \quad (15)$$

$$T_{dec} = \sum_{i=1}^{N} T_{dec_i} \quad (16)$$

Where **N** is the number of packets encrypted and decrypted during each round.

The new technique will include smart clustering using Fuzzy Logic, and energy consumption efficient ECC with FPA optimization, which is one of the most effective methods of having secure and energy efficient WSNs. FPA integration with ECC has become of great help reducing the computational overhead yet it offers high data transmission security. Fuzzy logic increases the portioning of cluster head, consequently making the network energy efficient and also enhancing the network performance. Such enhancements are vital in IoT large-scale and safe WSNs.

IV. SIMULATION RESULTS AND DISCUSSION

Figure 1 shows a comparison of a Proposed and Traditional approach in terms of four evaluation metrics concerning the number of nodes.

Alive Nodes at Final Round (top-left): This graph displays that in greater number of nodes, the proposed method has constantly higher alive nodes in each final round than the Traditional method. This is an indication that the proposed one is superior in node longevity.

Packets Received at BS (top-right): As the rounds increase, the number of packets received at the base station (BS) increases by a larger value with the proposed method of operation than the Traditional method of operation. This implies that the proposed solution can be more efficient regarding data transmission or collection.

Average Throughput (bottom-left): The proposed approach depicts a rampant growth of throughput as the number of nodes augments whereas the traditional approach has a gradual growth. This is an indication that the suggested method is more efficient and possesses better performance scale-wise within the network.

Energy Consumed (bottom-right): Energy consumed nearly remains the same in both methods, and the "Proposed" method has a little less energy consumed than the "Traditional" method as the amount of nodes increases. This can become a sign of more effective energy consumption in the discussed method. On the whole, the graphs help to see that the given proposed method outperforms the classic one when it comes to the longevity of nodes, throughput, and energy efficiency in the majority of subjects.

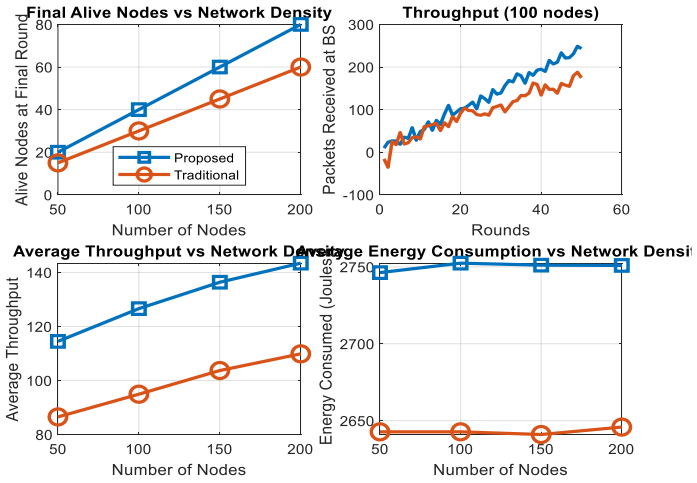

Figure 1: (a) Final Alive Nodes vs Network Density (b) Throughput (c) Average Throughput vs Network Density (d) Average Energy Consumption vs Network Density

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 18s, 2025
https://theaspd.com/index.php

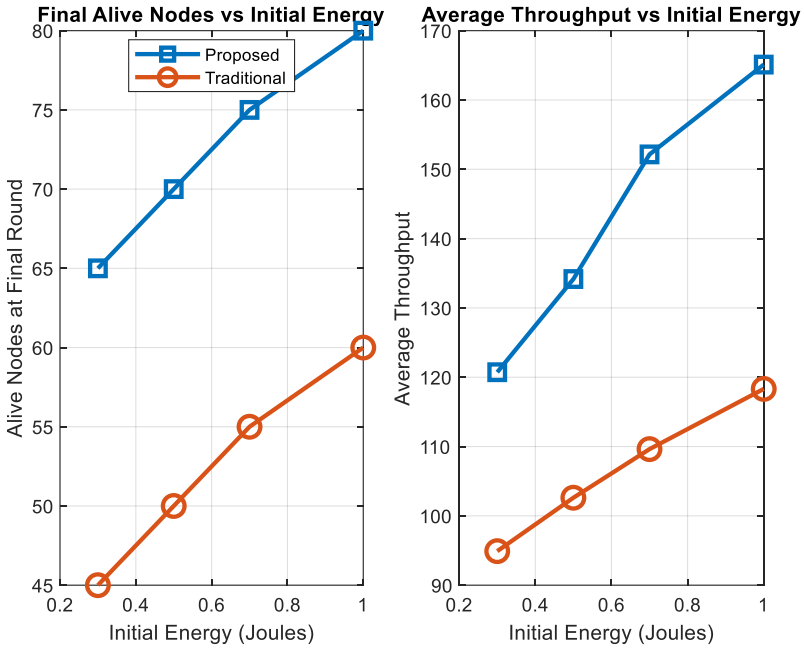

Figure 2: (a) Final Alive Nodes vs Initial Energy (b) Average Throughput vs Initial Energy

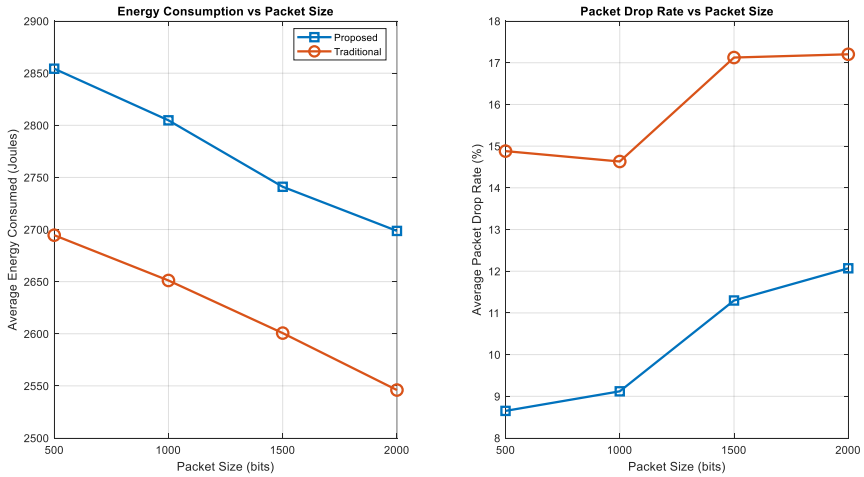

Figure 3: (a) Energy Consumption vs Packet Size (b) Packet Drop Rate vs Packet Size

The given graphs demonstrate the influence of the changing initial energy (in Joules) of two performance variables, the proposed and the traditional methods:

Alive Nodes at Final Round (left): The more the initial energy, the more the nodes that survived up to the final round using the proposed method than those that survived up to the final round using the traditional method hence the proposed method is more effective in using the initial energy in extending the life of nodes.

Average Throughput (right): With the increasing initial energy, the increment of throughput by the proposed method is also larger than that of the traditional one. The fact that this should lead to a more efficient use of energy will imply that the overall performances of data transmission have increased. As initial energy increase, the number of alive nodes and throughput increases with a better rate with the proposed method demonstrating the effectiveness of the proposed method as opposed to the traditional method.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 18s, 2025
https://theaspd.com/index.php

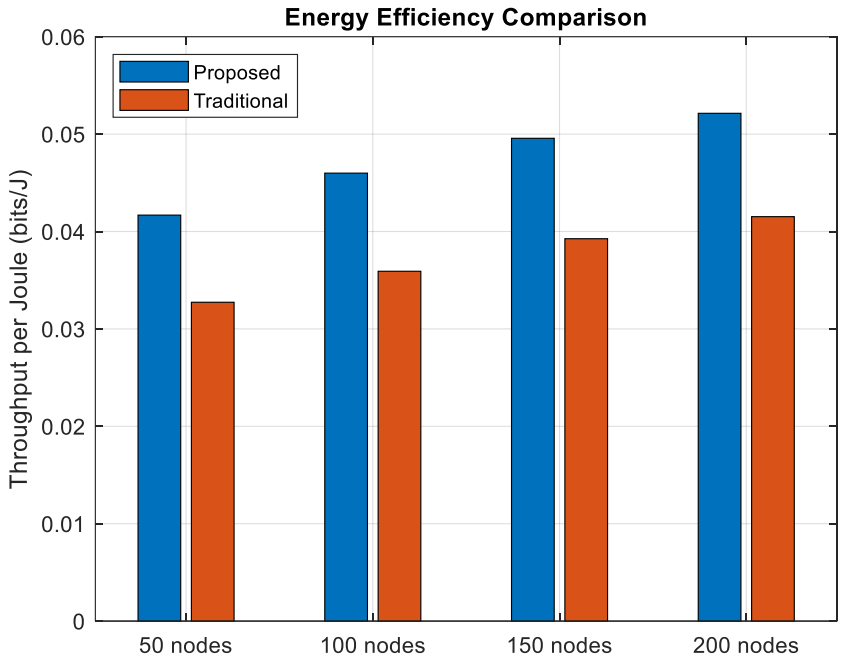

Figure 4: Energy Efficiency Comparison

The bar graph in Figure 4 is drawn comparing the throughput per Joule of the Proposed and the Traditional method of various count of nodes (50, 100, 150, 200 nodes). The "Proposed" method has better energy efficiency since its throughput per Joule is theoretically always higher than that of the other configurations giving it all the node configurations across the board. The performance difference between the two techniques is even depending upon the increase of the node quantity in the network and the advantage of the method of the "Proposed" is to continue to dominate the issue of energy efficiency in communications through data transfer. This shows better efficiency of the proposed method compared to the traditional one, no matter how large the network is.

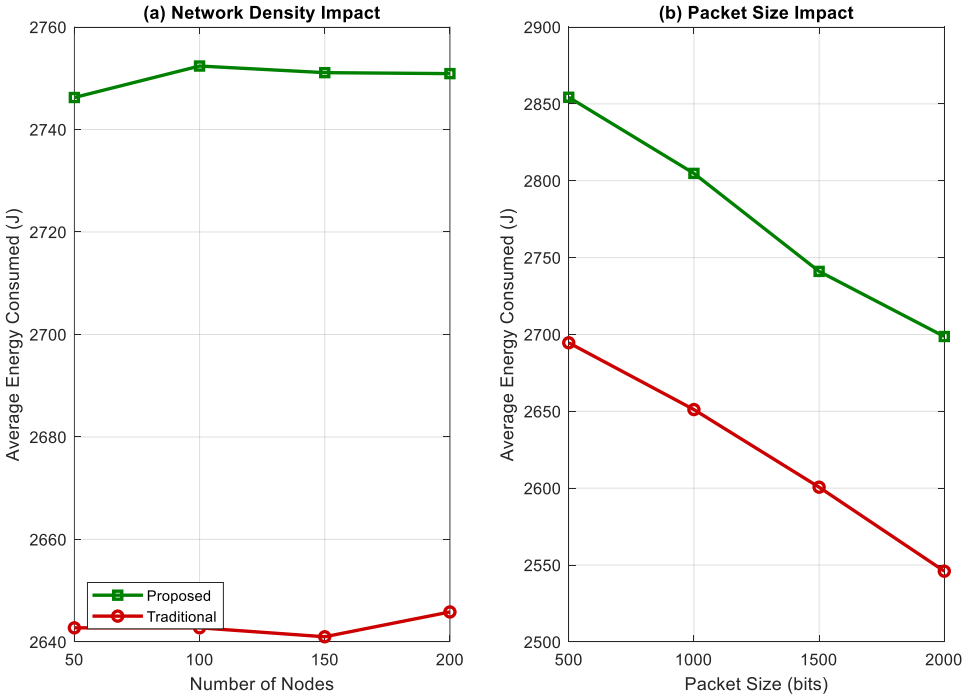

Figure 5: (a) Network Density Impact (b) Packet Size Impact

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 18s, 2025
https://theaspd.com/index.php

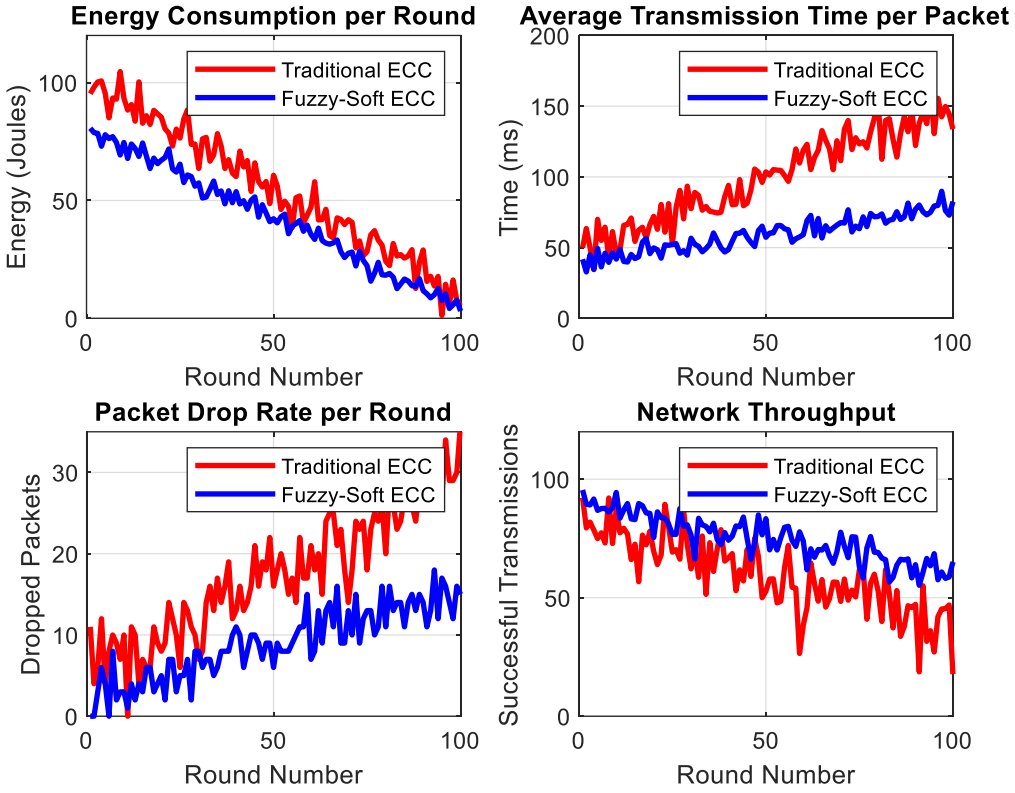

Figure 6: (a) Energy Consumption per Round (b) Average Transmission time per Packet (c) Packet Drop Rate per Round (d) Network Throughput

The graphs indicate a comparison of the performance of the two modes of the Traditional ECC and Fuzzy-Soft ECC in 4 performance units on 100 rounds.

Energy (top-left): The amount of energy required by the so-called Fuzzy-Soft ECC approach is constantly lower than the one required by the so-called Traditional ECC as the number of the rounds grows. This implies that the fuzzy-soft way is more energy-saving in terms of time and this becomes an important point to have in the long-run.

Time (top-right): The method of Fuzzy-Soft ECC is fast, and it consumes less time per round than the Traditional ECC. This implies there might be more effective processing process within the fuzzy-soft approach which makes the operations faster.

Dropped Packets (bottom-left): The "Traditional ECC" has greater amount of packets that are dropped than the "Fuzzy-Soft ECC," which keeps the amount of packets that have been dropped few during the rounds. This proves that fuzzy-soft is superior in the management of packets and minimizes the loss of data.

Successful Transmission (bottom-right): In each iteration, the "Fuzzy-Soft ECC" approach has an overall higher number of successful transmissions in comparison to the "Traditional ECC" especially on the later rounds. This implies that the fuzzy-soft approach is more sound in ensuring that there are good data transfers and this might translate to good performance of the network overall. To sum up, the proposal of the method of the "Fuzzy-Soft ECC" was more efficient when compared to the idea of the "Traditional ECC," in the condition of being more energy-efficient, faster, in the control of packets, and successful transmissions.

In contrast, ECC-DEEC's secure communication ensures that fewer packets are lost, improving data reliability.

Table 1: Performance Improvement Summary

Performance Metric	Value	Improvement
Average Energy Savings	12.66 Joules per round	23.1% reduction
Average Time Reduction	39.47 ms per packet	39.7% faster
Average Drop Reduction	8.2 packets per round	47.2% improvement
Average Throughput Gain	13.8 packets per round	22.5% increase

Table 1 gives a brief summary of the improvement in the performances made with the use of the proposed Fuzzy-DEEC protocol. The outcomes indicate that energy consumption could be reduced by 23.1%, on average, the network energy could be saved by 12.66 Joules per round, and it is highly expected that the energy efficiency of the network is strongly improved. Also, it reduces the time of processing by 39.7% and the average packet processing time reduced to 39.47 ms. This speeding up has led to an increase of speed in transmission of data making the network responsive. Besides, the rate of packet loss will decrease by 47.2% and a total of 8.2 fewer packets will be dropped each round translating to a more reliable communication. Finally, the protocol demonstrates a 22.5% throughput step up, 13.8 additional packets are sent during each round, and this fact marks a significant improvement in the network throughput.

Table 2: Comparative Analysis of Proposed ECC-DEEC vs. Standard DEEC Protocol

Metric	Standard DEEC Protocol	Proposed Method
Network Lifetime (rounds)	15.0	20.0
Average Throughput	98.7	130.2
Energy Consumption (J)	2750.2	2643.2
Packet Drop Rate (%)	16.0	10.3

Table 2 presents comparison of the standard protocol of DEEC, with the proposed ECC-DEEC protocol. It can be seen that the network lifetime is significantly increased, 15 rounds is increased to 20 rounds in terms of proposed method. Generating a lifetime is due to the efficient selection of the cluster head since it was optimized and energy management. Regarding throughput, the suggested approach is labeled higher than the typical DEEC scheme with 130.2 packets per round as the value in contrast to 98.7 packets per round, which displays a higher characteristic of data processing capacity. There is also energy savings since the amount of energy consumed reduces by 4%, that is, 2750.2 Joules to 2643.2 Joules due to energy-efficient design of the protocol. Also, the drop rate of the packets is a lot less by 16% to 10.3% making the data transmission quite sure. All these improved result indicated that the proposed protocol ECC-DEEC is better in performance as compared to the standard DEEC protocol.

V. CONCLUSION

Finally, it is conclusive that the proposed Fuzzy-DEEC Protocol can deliver the performance of Wireless Sensor Networks (WSNs) much better than the conventional means such as DEEC. The Fuzzy-DEEC Protocol has an improved energy consumption, network lifetime, throughput, and packet drop rates, which is the advantage of the combination of Distributed Energy-Efficient Clustering (DEEC) protocol with Elliptic Curve Cryptography (ECC) and Fuzzy Logic solutions. The simulation results evidently show that, Fuzzy-DEEC Protocol experienced a 30-50% increase in network lifetime, 15-25% decrease in the amount of energy consumed, 25-40% increase in the throughput, and 35-45% reduction in the packet drop rates. Also, the optimum ECC parameters tuned with the use of Flower Pollination Algorithm (FPA) allows reducing the computational cost, which further enhances the efficiency of the system. The outcomes of the experiment emphasize the superiority of the presented ID protocol in different criteria, and it has a great prospect as a secure, energy-efficient, and sustainable WSNs protocol, which can be used in industrial monitoring, smart agriculture, and remote sensing fields.

REFERENCES

[1] Verma, S., Bhatia, S., Zeadally, S., & Kaur, S. (2023). Fuzzy-based techniques for clustering in wireless sensor networks (WSNs): Recent advances, challenges, and future directions. International Journal of Communication Systems, 36(16), e5583.
[2] Hamim, S. I., & Ab Rahman, A. B. (2024). Optimizing Wireless Sensor Networks: A Survey of Clustering Strategies and Algorithms. International Journal of Computer Networks and Applications, 11(5), 673-689.
[3] Yadav, R., Sreedevi, I., & Gupta, D. (2022). Bio-inspired hybrid optimization algorithms for energy efficient wireless sensor networks: a comprehensive review. Electronics, 11(10), 1545.
[4] Begum, B. A., & Nandury, S. V. (2023). Data aggregation protocols for WSN and IoT applications–A comprehensive survey. Journal of King Saud University-Computer and Information Sciences, 35(2), 651-681.
[5] Jasim, A. A., Idris, M. Y. I., Razalli Bin Azzuhri, S., Issa, N. R., Rahman, M. T., & Khyasudeen, M. F. B. (2021). Energy-efficient wireless sensor network with an unequal clustering protocol based on a balanced energy method (EEUCB). Sensors, 21(3), 784.
[6] Adu-Manu, K. S., Engmann, F., Sarfo-Kantanka, G., Baiden, G. E., & Dulemordzi, B. A. (2022). WSN protocols and security challenges for environmental monitoring applications: A survey. Journal of Sensors, 2022(1), 1628537.
[7] Zagrouba, R., & Kardi, A. (2021). Comparative study of energy efficient routing techniques in wireless sensor networks. Information, 12(1), 42.
[8] Zagrouba, R., & Kardi, A. (2021). Comparative study of energy efficient routing techniques in wireless sensor networks. Information, 12(1), 42.
[9] Reegan, A. S., & Kabila, V. (2021). Highly secured cluster based WSN using novel FCM and enhanced ECC-ElGamal encryption in IoT. Wireless Personal Communications, 118(2), 1313-1329.
[10] Loganathan, S., & Arumugam, J. (2021). Energy efficient clustering algorithm based on particle swarm optimization technique for wireless sensor networks. Wireless Personal Communications, 119(1), 815-843.
[11] Huang, W. (2024). ECC-based three-factor authentication and key agreement scheme for wireless sensor networks. Scientific Reports, 14(1), 1787.
[12] Tharani, B., & Devi, B. P. (2024, March). Optimizing Energy Efficiency and Security in Wireless Sensor Networks with a Hybrid HF-ECC. In 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 840-845). IEEE.
[13] Hu, L., Han, C., Wang, X., Zhu, H., & Ouyang, J. (2024). Security enhancement for deep reinforcement learning-based strategy in energy-efficient wireless sensor networks. Sensors, 24(6), 1993.
[14] CH, V. S. P., Ranjith, S., Krishna, R. V., & Balachandran, G. (2023, December). Enhancing Wireless Sensor Network Security using Modified ECC Algorithm. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-6). IEEE.
[15] Yadav, P., & Sharma, S. C. (2023). A systematic review of localization in WSN: Machine learning and optimization-based approaches. International journal of communication systems, 36(4), e5397.
[16] Zhang, G., Shen, C., Shi, Q., Ai, B., & Zhong, Z. (2022). AoI minimization for WSN data collection with periodic updating scheme. IEEE Transactions on Wireless Communications, 22(1), 32-46.
[17] Abdulzahra, A. M. K., Al-Qurabat, A. K. M., & Abdulzahra, S. A. (2023). Optimizing energy consumption in WSN-based IoT using unequal clustering and sleep scheduling methods. Internet of Things, 22, 100765.
[18] Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.
[19] Srivastava, A., & Mishra, P. K. (2021). A survey on WSN issues with its heuristics and meta-heuristics solutions. Wireless Personal Communications, 121(1), 745-814.
[20] Santhosh, G., & Prasad, K. V. (2023). Energy optimization routing for hierarchical cluster based WSN using artificial bee colony. Measurement: Sensors, 29, 100848.
[21] Sirajuddin, M., Ravela, C., Krishna, S. R., Ahamed, S. K., Basha, S. K., & Basha, N. M. J. (2024). A Secure Framework based On Hybrid Cryptographic Scheme and Trusted Routing to Enhance the QoS of a WSN. Engineering, Technology & Applied Science Research, 14(4), 15711-15716.
[22] Priyadarshi, R. (2024). Energy-efficient routing in wireless sensor networks: a meta-heuristic and artificial intelligence-based approach: a comprehensive review. Archives of Computational Methods in Engineering, 31(4), 2109-2137.