Efficient Cluster Head Selection And Secured Routing Using Distribution Based Chicken Swarm Optimization Algorithm And Elliptic Curve Cryptography Over Iot-Wsn

[1*]Dr A. Prakash and [2]M. Prakash

[1]Professor, Department of Computer Applications (PG), Hindusthan College of Arts &amp; Science. Coimbatore.*

[2]Research Scholar, Department of Computer Science, Hindusthan College of Arts &amp; Science. Coimbatore.

Abstract

IoT (Internet of Things) uses WSNs (wireless sensor networks) to obtainenvironment data and send them to base stations, and other locations for evaluations. Intelligent routing is a significant thing in WSNs for IoT that is required to strengthen the network's Quality of Service (QoS). In addition, IoT-based sensor networks' energy requirements making it complex to eliminate packet losses or drops, rapid energies depletions, and all of which can lower node efficiencies and extend packet deliveries. Therefore, it is essential to keep an eye on node energy consumption in order to use intelligent learning techniques for intelligent routing decision-making and enhance network performance as a whole. This paper suggests the use of the ECC (Elliptic Curve Cryptography) technology and the DCSO (Distribution based Chicken Swarm Optimisation) algorithm for safe multipath routing via IoT-based WSN. This work includes system model, CH (Cluster Head) node selection, fault-tolerance based secured multipath routing withencryption process. In this study, optimal CH node selection is achieved by utilizing DCSO algorithm which is used to increase the speed of the data transmission and energy efficiency through best fitness function values.The secured data transmission is achieved by removing the sinkhole attack nodes effectively using ECC technique which is employed to boost the security level for fast data transmission over routing on IoT based WSN. The result proves that the suggestedDCSO-ECCframework provides better performance in terms of higher throughputs, rates of data transfers, network lifetime and reduce energy consumptions than existing methods

Key words: *Wireless Sensor Networks (WSNs), Internet of Things , Distribution based Chicken Swarm Optimization (DCSO) algorithm and Elliptic Curve Cryptography (ECC)*

1. Introduction

IoT devices with limited storage and energy options can access sensing services from WSNs , which are collections of specialized transducers. Power conservation becomes the main design factors in WSN because changing or recharging the sensor nodes' batteries is practically impossible [1]. For the energy-constrained network, clustering algorithms are crucial for power conservation. By carefully balancing the network's demand, a CH can lower energy usage and extend lifespan. IoT comprises of intelligent devices (sensor nodes) in WSNs. These nodes have a limited amount of energy, computational, memory, and processing capability, hence they are arranged at random to gather data [2]. Network attacks can undermine communication in Internet of Things

(IoT) systems because of the intricate structure of WSN and the loose restrictions on sensor nodes. Fig. 1 describes the IoT-based WSN architecture.

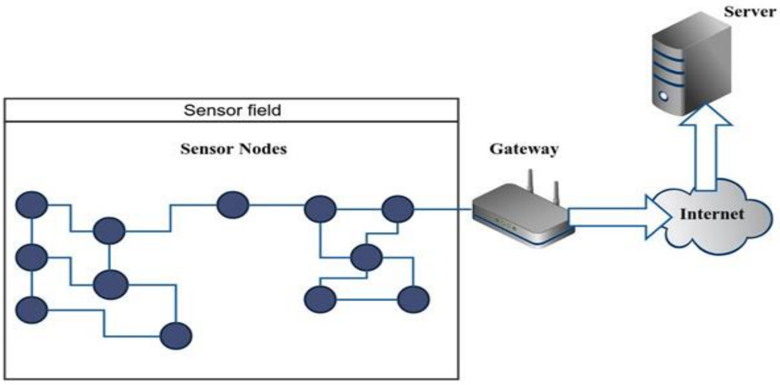

Fig 1 IoT based WSN architecture

The integration and communication of smart devices has been described as the IoT. As a result of IoT's domination, new apps and services are emerging. Wireless and wired networks connect a variety of devices, with sensors, Radio Frequency Identification (RFID) tags. Smart devices can perceive, gather, and transfer data to meet the diverse needs of people. Additionally, WSNs can be used tomonitorwater qualities or in smart citiesetc. In addition to dependable data forwarding, improving energy efficiency [3] is a crucial issue. A cluster-based WSN solution has already been proposed by many academics for improving energy efficiency [4].

The nodes are divided into several regions using clustering techniques, with one CH being elevated to the position of leader node. The CH's job is to gather information from member nodes, combine it, and send it over one or more hops to the BS. There are two primary categories of clustering solutions: probabilistic and non-probabilistic approaches. Clusters are created randomly in probabilistic [5], which leads to an imbalanced load distribution and energy usage. Non-probabilistic techniques, choose CHs based on a variety of parameters. Because sensor nodes are dynamic, non-probabilistic algorithms perform better than standard probabilistic methods; yet, improving energy conservation and routing resilience remains a challenge for IoT based on WSN.

Low and limited power sources that are non-replaceable are carried by sensor nodes. Thus, creating an improved QoS-based, energy-efficient WSN protocol is a challenge academics face. The data collection and routing process consumes the greatest energy in a sensor network when compared to other tasks [6]. Researchers have employed a variety of routing protocols that primarily focus on determining best routes amongst sources and destinations while examining QoS characteristics likereliability, throughputs, or delays.

The main aim of this research work is fault-tolerance based multipath routing and CH node selection on IoT based WSN. The current methods have issues with PDR measurements and energy use. The DCSO-ECC model is employed to develop the efficiency of the system in WSN in order to address the problems. The primary advantage of this study is construction of system model,CH node selection and fault-tolerance based secured multipath routing. The suggested approach uses powerful algorithms for the cloud environment to give improved performance.

The other segments of the paper are structured as follows: In Section 2, some research on secured multipath routing and CH node selection in the literature is provided. Section 3 contains more details on the recommended technique for the DCSO-ECC technique. The results of the study and simulation are presented in Section 4. In Section 5, the conclusions are compiled.

2. Related work

In [7], John et al (2017) suggested CHswith energy efficiency that improve lifespan of sensor nodes used for sensing. These sensor nodes must conserve energy if they are to prevent rapid battery loss. The network lifetime created for IoT applications is therefore improved by the energy-saving CH selection (ESCHS) technique. For cluster formation, this technique uses the concept of uniform clustering. Utilizing each sensor node's remaining energy, CH is selected. To qualify as CH, a node must have residual energy greater than the average residual energies of relevant clusters. Theiroutcomes demonstrated the suggestedmethods work better thanexisting techniques in energy conservations and durability of networks.

In [8], Wang et al (2018) suggested a clustered routing technique with low energy consumption. Due to unequal distributions of traffic, they employed tactics for unequal cluster formation to achieve energy efficiency and load balancing. Distributed rotation methods of CH were also employed to maintain equilibrium in energy consumption across clusters. They developed energy-aware cost functions and dynamic multi-hop routing strategies between CH nodes to address energy hole problems for long-distance transmissions to BS. The accuracy of the method is competitive with regard to of network longevity, throughput, according to simulation findings.

In [9], Rani et al (2015) suggested a creative deployment strategy to address concerns with energy efficiency. This plan introduces: (1) Designing hierarchical networks (2) IoT models for energyefficiencies; and (3) transmissions with minimal energy consumptions for executing top models into practice. It is now easier to create IoT energy-efficient systems. The findings demonstrate that the novel method is more flexible and energy-efficient than previous WSN schemes, allowing for effective IoT connectivity.

In [10], Mahajan et al. (2014) employed the Cluster Chain Weight Metrics approach (CCWM), a method for selecting CH weights that takes service aspects into account for increasin g network efficiency. Selecting the appropriate CHs for the network and forming balanced clusters are two of the main problems with a clustering-based approach. The first step in creating a cluster in a network is to choose the CHs based on a weight measure. This technique maintains sensor energy while also balancing load. A local clustering technique is applied within the cluster to reduce computation and communication expenses. A unique data transport technique is also looked into.

In [11], Saidi et al (2020) offered a technique for detecting misbehaviour and a trustworthy CH election procedure. For CH elections, key performance indicators like as trust ratings of sensor nodes were used. The problem of choosing a trustworthy node to act as CH was also taken into consideration. Furthermore, a monitoring method was developed to evaluate the behaviour of sensor nodes using a range of trust types. Therefore, the objective was to remove all malicious nodes from the network while maintaining just the reliable nodes. In the event of a compromised CH, a system for evaluating member trust and a local clustering strategy were developed to isolate the malicious CH without compromising network performance.The outcomes show that the strategy shields the network from tainted CH following the election and stops malevolent nodes from evolving into CHs. The method detected hostile nodes with a high rate of misbehaviour and a low quantity of false positive and false negative alerts.

In [12], Agarkhed et al (2021) introduced nodes with smallest overall delays and congestion indices are chosen as the CH using best CH selection approaches. The next rounds CH were determined by nodes that have greatest energies remaining and are not currently suffering delays or high traffics. Energy and congestion indices cost functions are used to build inter-cluster routing paths, which result in multipaths and aggregated bandwidths. It is possible to allow adaptive CH and route selections, and QoS settings may be changed to suit application needs. The technique beatexisting protocols in terms of low energy consumptions, low packet loss ratios, and high throughputs.

3. Proposed methodology

Here, DCSO-ECC algorithm is proposed to enhance the CH node selection and fault tolerance based secured multipath routing over the IoT based WSN. The main contribution of this research is system model, CH node selections via DCSO algorithm, routing processes and secured data transmissions using fault tolerance mechanisms and ECC algorithm. The suggested method's main block diagram is presented in Fig. 2.

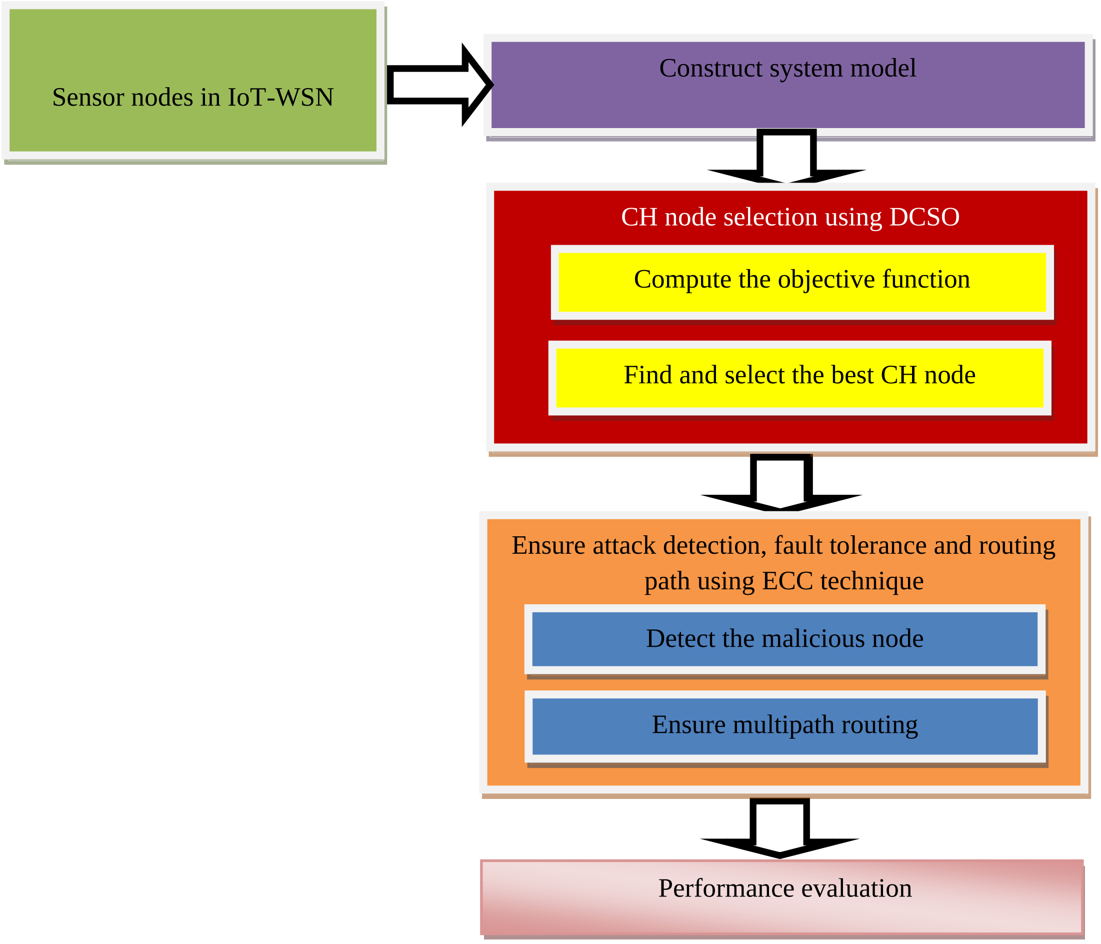
Sensor nodes in IoT-WSN
Construct system model
CH node selection using DCSO
Compute the objective function
Find and select the best CH node
Ensure attack detection, fault tolerance and routing path using ECC technique
Detect the malicious node
Ensure multipath routing
Performance evaluation

Fig 2 Overall block diagram of the proposed system

3.1 System model

WSN is an essential component of IoT in the environmental monitoring scenario presented in this section. The network's sensor nodes are arranged into many groups known as clusters. Each one also consists of a CH and a few member nodes. Each member node in the bottom layer is in charge of data sensing for interest. There should only be one sensor node in any collection of nodes that can function as the CH at any one time. The fused data that the sink node collected from each group's CHs is sent to the end user. The routing backbone is built by the intermediate layer CHs in order to gather, aggregate, and transfer data from member nodes. The base station at the top layer transmits data from CHs to the server. This system enables low-power and scalable Internet of Things. This design may be used to effectively retain energy by placing IoT components on top of it. The Internet of Things (IoT) network is represented by the symbol G(N,V), where N denotes the set of all nodes in the area and V denotes the set of wireless links connecting the nodes. The letters R represent the relay nodes' communication radius, whereas r stands for the local nodes.

3.2 Radio model

Interferences cause differences in the channel characteristics of open wireless media. Markov chains in two states are then used in this study to simulate these time-varying wireless media. $S = \{s0, s1\}$ [13].

where, s0 and s1 represent good and bed states of the channel quality respectively. The random variable with an exponential distribution is the channel quality time interval (t) between each state..

$$p(t) = \begin{cases} \alpha_i e^{-\alpha_i{}^{t}} t \geq 0 \\ 0 \qquad t < 0 \end{cases} \qquad (1)$$

here $\alpha_i, i \in \{0,1\}$ are the rates of good and bad states. The probability that the channel state will change from bad to excellent is then determined by $p_0 = \alpha_0/(\alpha_0 + \alpha_1)\ and\ p_1 = \alpha_1/(\alpha_0 + \alpha_1)$correspondingly

The wireless transmission loss can be represented by either the two-ray ground reflection model or the free-space propagation model, depending on the distance between the transmitter and receiver. The first model fits the gearbox loss better if d is smaller than a predefined threshold, d_0. In all other cases, the second model ought to be applied. The threshold d_0 in this example may be found using

$$d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{amp}} \tag{2}$$

here $\varepsilon_{fs}$and $\varepsilon_{amp}$are the amplified characteristic constants involving the transmission loss models

The amount of energy used by a node to send a k-bit data packet over distance d can be stated as

$$E_{Tx}(k,d) = \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, & d < d_0 \\ kE_{elec} + k\varepsilon_{amp}d^4, & d \geq d_0 \end{cases} \tag{3}$$

where E_{elec} stands for energies spent by transmitters or receiver circuitries

used energies by receivers for k-bit data packets can be measured by

$$E_{Rx}(k) = kE_{elec} + kE_{DA} \tag{4}$$

where $E_{DA}$is the energy spent by the receiver for aggregating a one-bit packet

3.3 Security model

This work proposes a trust-based security architecture that includes fuzzy trust evaluation, trust grouping, outlier identification, trust evidence collecting, and trust recommendation to avoid attacks in resource-constrained WSNs. Each sensor node regularly gathers the trust evidences of other nodes by listening to broadcasts in order to construct a trust-based secure system. After the evidences are updated, an IT2 fuzzy logic system (FLS) is built to successfully reduce the uncertainty of the trust evidences and calculate the trust values by fuzzy inferring. Using each node in the trust recommendation process allows it to accrue a significant amount of trust values. Trust grouping is then used to investigate these values in more detail. Group means are then used to identify the outliers, and a node's maliciousness can be determined.

3.4 Cluster formation and CH node selection using DCSO algorithm

In IoT-based WSNs, clustering is a practical procedure used to safeguard sensor nodes' battery life. The high energy efficiency of clustering extends the lifetime of WSNs. The following are some benefits of WSN clustering: high level of energy economy (i). (ii)Cumulative or condensed data is sent directly between CH and BS to reduce the number of broadcast nodes linking BS. Sensor nodes are divided into virtual groupings known as clusters during the clustering process, and each cluster's nodes perform a variety of activities. As per the concept of clustering, nodes are categorised into groups based on specific attributes, and the most productive node within each group is designated as the CH.

Utilizing the DCSO method on the IoT-based WSN, CH nodes are chosen in this phase. CSO method is used to extract the swarm intelligence of chickens to solve issues by emulating their hierarchical structure and behaviours, including roosters, hens, and chicks. DCSO is therefore used in CH node selection to discover the best node groupings to improve IoT-based WSN efficiency. The algorithm imitates hierarchies of chicken swarms and individual chickens' behaviours. The hierarchy of a swarm of chickens divides into numerous groups, each consisting of a rooster, several hens, and chicks. distinct kinds of chickens are subject to distinct laws of motion. Hierarchical order plays a key role in hens' social interactions. The most powerful chickens in a flock will subjugate the weaker ones. Submissive hens stand outside the groupings, while more dominant hens kept closer to the roosters. The nature of the CSO algorithm is seen in Fig. 3.

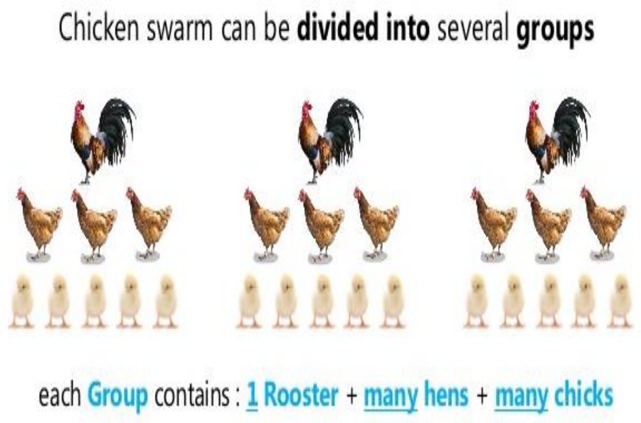
Chicken swarm can be divided into several groups
each Group contains : 1 Rooster + many hens + many chicks

Fig 3 Nature of CSO algorithm

Chickens Movements

Rooster Movement: Better-fit roosters have a larger range of locations where they can look for food.

Hen movement: Hens in a flock follow the roosters to locate food. The other chickens would also put restrictions on them, but they would heedlessly pilfer the delicious food the other birds had discovered. When it came to the struggle for food, the stronger chickens would win out over the weaker ones.

Chick movement: In order to find nourishment, the chicks roam about their mother.

The regulations that follow explain the actions of the chickens and provide the foundation of the mathematical model of CSO utilized in [14]:

1) chicken swarms have different groups. There are dominant roosters in groups, proceeded by several hens and chicks.

2) The roosters which act as group leaders have the maximum fitnesses, while chicks have least fitnesses, illuminating the organizational structure of the swarm. The hens would be the other group.

3) The mother-child relationship and the group's power dynamics won't change. Only a few time steps separate updates for these states.

4) The virtual chickens in the swarm are separated into n groups as follows: R_n, C_n, $H_n$and M_n which are counts of roosters, chicks,hens, and the mother hens, correspondingly. The positions of each individual in a D-dimensional space serve as a representation of

$$x_{i,j}(i \in [1,\ldots,N], j \in [1,\ldots,D]). \tag{5}$$

Greater fitness values are given preference over lower fitness standards in terms of feeding roosters. The fact that roosters with higher fitness values can forage in a wider range of environments than roosters with lower fitness values makes it easy to replicate the situation. The use of the Gaussian distribution helps to greatly reduce mistake rates because the normal CSO has a problem with them. The DCSO may then be created as shown below.

$$x_{i,j}^{t+1} = x_{i,j}^{t} * (1 + Randn(0, \sigma^2)) \tag{6}$$

$$\sigma^2 = \begin{cases} 1, \ if\ f_i \le f_k & k\epsilon[1,N], k \ne i \\ \exp\left(\frac{(f_k - f_i)}{|f_i| + \varepsilon}\right), & \text{otherwise} \end{cases} \tag{7}$$

Where Randn (0, σ^2) are Gaussian distributions with means 0 and standard deviationsσ^2, The lowest constant, ε, is employed to avoid mistakes in zero-division calculations. The term "f" denotes matching x's fitness levels, and the indices of the roosters are randomly picked among groups of roosters.

The roosters lead the hens in their flock on a food hunt. Additionally, they would clumsily steal the delectable food that other had found even when restricted by the other chickens. The superior hens would profit from food competition in contrast to more submissive birds. These issues can be formally expressed as follows.

$$x_{i,j}^{t+1} = x_{i,j}^{t} + S_1 * rand * \left(x_{r1,j}^{t} - x_{i,j}^{t}\right) + S_2 * rand * (x_{r2,j}^{t} - x_{i,j}^{t}) \quad (8)$$

$$S_1 = \exp\left((f_i - f_{r1})/(abs(f_i) + \varepsilon\right) \quad (9)$$

$$S_2 = \exp\left((f_{r2} - f_i)\right) \quad (10)$$

rand is a consistent random number between [0, 1], where. While $r2\epsilon[1, .. N]$ is an index of the chicken, which is randomly chosen from the swarm $r1 \neq r2$, $r1\epsilon[1, .. N]$ is a representation of the rooster, the ith hen's groupmate.

Of course, $f_i > f_{r1}, f_i > f_{r2}$,, therefore S2 <1< S1. Assuming S1=0, the ith hen would feed for food before the other chickens. Greater fitness value and lower S2 are seen between two chicks whose locations are more dissimilar from one another. Thus, There would be a reduced likelihood of the chickens stealing food found by other birds. As a result of intragroup contests, S1's formula form differs from S2's.To make things simpler, the contests amongst hens in a set are represented by the chickens' fitness values in relation to the rooster's fitness value. When S2 is equal to zero Within its own domain, the ith hen would look for food. For that group, the rooster has a unique fitness value [15]. Thus, the more S1 resembles 1 and the closer its position is to that of its groupmate rooster, the lower the ith hen's fitness value. Consequently, the stronger hens are more likely than the weaker birds to take the food.

Young birds move around their mother to discover nourishment which is presented as follows

$$x_{i,j}^{t+1} = x_{i,j}^{t} + FL * \left(x_{m,j}^{t} - x_{i,j}^{t}\right) \quad (11)$$

Where $x_{m,j}^{t}$ are positions of ith chick's mothers ($m\epsilon[1, N]$). $FL(FL\epsilon(0,2))$ are parameters, suggests that chicks might go hunting with their mothers. Given variations in chicks, FL would randomly select numbers amongst 0 and 2.

Algorithm 1: DCSO

Input: a population of $n$chickens (IoT based WSN)

Objective: Best solution (higher data transfer rate and lower energy consumption)

Output: Optimal CH node selection

```
Initialize the parameters such as $R_n$, $H_n C_n$, and $M_n$
Estimates N chickens' fitness values, t=0; (higher data transfer rate and lower energy consumption)
While $t < Maximum$ iteration do
    If t%G==0 then
        Ranks nodes' fitness values and create hierarchal orders in swarms
        Separate swarms into various groups and ascertain how each groups' mothers and chicks are related to one another.
    End
    For i=1 to N nodes (data transfer rate and lower energy consumption) do
        If i==rooster then
            Update the solution using (6)
        End if
        If i==hen then
            Update the solution using (8)
        End if
        If i==chick
            Update the solution using (11)
```

```
End if
Estimate the novel solution
Update it if the newly created solution is superior to the prior one.
End
End
Return $x_{best}$ (better CH node selection)
```

Here, utilizing the sensor nodes' arbitrary positions as a means of allocating and identifying the chicks. The highest fitness chicken is updated to enhance the key node of the Algorithm 1-described IoT-based WSN. Using equation (11), determine the best hens (CH nodes) with global best food searches for fitness values by computing best values for all chickens (sensor nodes). The DCSO method is used in the suggested framework to identify node combinations that enhance IoT-based WSN efficiency with a minimum amount of hop counts. DCSO considers the parameters are such as lower energy consumption and higher data transfer rate nodes which selects the best CH node over the given IoT based WSN.

3.5 Fault tolerance mechanism for energy aware routing and ECC technique for security

The fault tolerance and robustness over IoT based WSN are handled by the fault tolerance based Dynamic Source Routing (DSR) routing protocol. By designing a backup route for each node on the primary line of data transmission, it created the fault tolerance mechanism. The node directly transmits the incoming data packets using its backup route rather than the earlier broken route, maintaining continuity of data packet delivery and reducing the number of decreased data packets from path failure when there are faults on the main path of data transmission.

Multipath routing among participating nodes that want to create and maintain a fault-tolerant WSN is made possible by the suggested fault tolerance centered DSR routing protocol. DSR enables the construction of routes among nodes that want to communicate quickly and effectively [16]. A path's hop count serves as a criterion for path selection. The route with the fewest hops is chosen if the source receives several RREPs with the same destination sequence number.

To increase security and effectively identify attacks during data transfer via IoT-based WSN, ECC is introduced. Each user taking part in the communication often has a set of actions connected to the keys, a public key, and a private key to carry out the cryptographic operations. The term "public key cryptography" applies here. The public key is available to everyone in the chat, but the private key is only accessible by a single user.It is employed to produce cryptographic keys more quickly, compactly, and effectively [17].

An instance of a routing attack known as a sinkhole includes at least one rogue node [18]. Typically, it announces to the target node that it has a superior data send route. The attack's malicious node, which has the ability to alter the network's routing protocol, is typically placed close to the Sink node. It results in data packets being transferred to malicious nodes when they should have been delivered to the sink node. The malicious nodes just need to offer a high-quality link to the BS because all the packets share the same endpoint due to the unique transmission mechanism of WSNs.

To overcome the above mentioned problem, ECC is introduced which provide better security. In the ECC method, With the recipient's public key for encryption and private key for decryption, the sender encrypts the message. choose a number 'd' from the range of 'n'. With the help of the subsequent equation, it can produce the public key.

$$Q = d * p \tag{11}$$

where, d = The random number chosen within the range of (1 to n-1).

p= the point on the curve. Q = the public key and d is the private key

Although the suggested technique encrypts all incoming sensed data from the sensor nodes using the ECC method, which employs ECC cryptography for IDs. As a result, the method yields superior results regarding energy utilisation. Unlike the data and status response messages sent to the CH, the sensor node only sent a single message with all the information needed for verification to the CH. The results demonstrate that this tactic has completely succeeded in securing the network.

A node uses its encrypted ID to send a message to other sensor nodes if it turns into a sinkhole attacker. The sender-node encrypted ID is given to the CH for authentication when the other nodes get this message. After decrypting the ID with Keyn, the CH treats the node as an attacker if it discovers that the ID belongs to a sensor node rather than a CH or that the node is a member of a lower-level cluster. The attack node is subsequently cut off from communication by the CH, which immediately notifies the base of separation (BS) of the attack and provides the attacker's ID in an alarm message. The CH then sends a Negative Acknowledgement message (NACK) to the receiving node.

As an outcome, there will be significantly stronger privacy because the attacker won't be capable of eavesdrop on the data from intermediate nodes. It offers protection from a variety of attacks, including changing the routing data, selective forwarding, sinkhole, wormhole, and Sybil attacks, among others. Additionally, it employs encryption as a security feature to safeguard messages. In order to ensure secure data transit from sensor nodes to BS, the recommended schema is used.

4. Simulation result

The utility of the recommended DCSO-ECC technique is examined and evaluated against earlier techniques like Evolutionary Game based Secure Clustering protocol with Fuzzy trust evaluation and Outlier detection (EGSCFO) [19] scheme, Taylor Kernel Fuzzy C-means Clustering (TKFCC) [20], Weight Red Deer Algorithm (WRDA) andImproved Butterfly Optimization (IBO) Algorithmand Double key based Advanced Encryption Standard (DAES) algorithms.The settings for the simulation are listed in Table 1, and the NS-2 tool is used to simulate this research. The throughputs,energy consumptions, data transfer rates and network lifetimeof the suggested and current techniques are evaluated.

Table 1: simulation parameters

Parameter	**values**
Counts of Nodes	100
Sizes of Areas	1100 * 1100(Meter)
Mac	802.11
Sum of energy	150 Joule
Energy’s initial Value	1.5 Joule
Radio Ranges	250m
Simulation Times	60 sec
Sizes of Packets	80 bytes

Throughput

The speed at which data packets go over a network or communication channel is known as throughput.

$$Throughput = total\ number\ of\ packets\ sent\ /time \qquad (12)$$

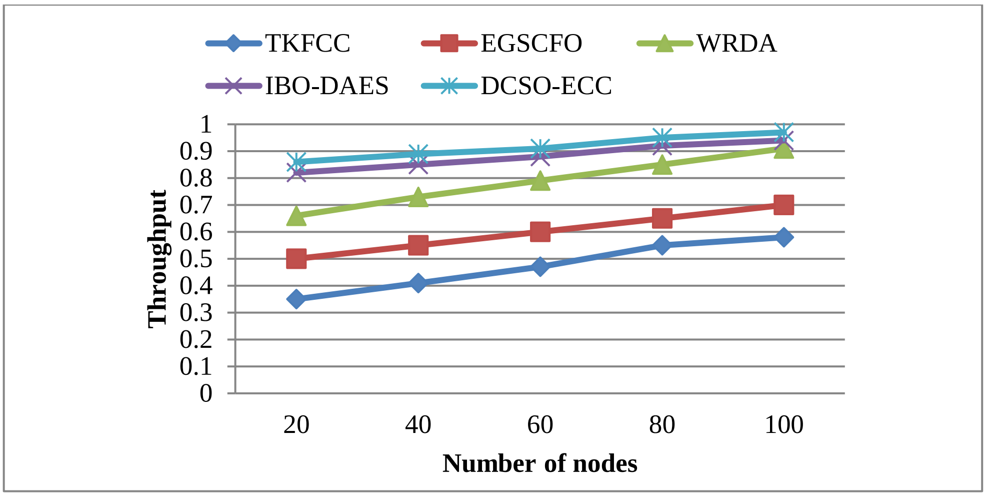

Fig 4 Throughput comparison

Fig 4 shows how the current TKFCC, EGSCFO, WRDA, IBO-DAES, and IBO-DAES approaches compare with one another on the throughput measure. The x-axis represents node counts, whereas the y-axis represents throughputs. The suggestedDCSO-ECC method is utilized to determine and select the CH nodes effectively in WSN. Additionally, because there are fewer nodes participating in cluster communication, there is less packet loss, which helps to increase throughput to a much higher level. This helps to accurately gather and transmit the secured data in different node without any information loss. It shows that the existing TKFCC, EGSCFO, WRDA, IBO-DAES techniques offer a lesser throughput compared to the suggested DCSO-ECC solution.

Energy consumption

Energy consumption is the average amount of energy needed over time for sending, receiving, or forwarding a packet to a network node.

$$Energy\ (e) = [(2 * pi - 1)(e_t + e_r)d \qquad (13)$$

The data packet is represented by pi in this equation, together with the energy needed to send packet I, the energy needed to receive packet I, and the distance between nodes at the source or destination by d..

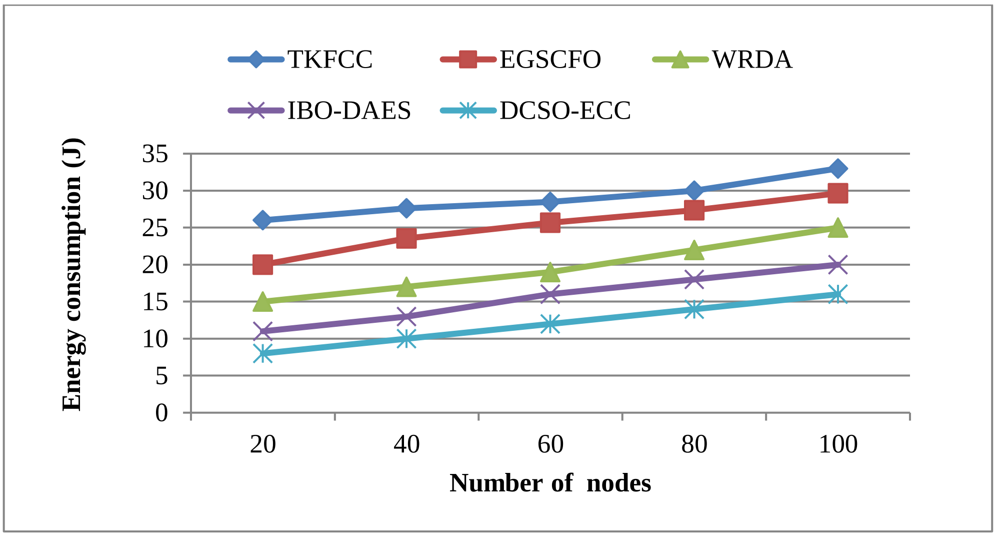

Fig 5 Energy consumption comparison

The comparison of energy consumption utilizing the DCSO-ECC algorithms suggested by IBO-DAES, TKFCC, EGSCFO, WRDA, and current methods might be shown in Fig. 5. The x-axis counts the number of nodes, while the y-axis measures the energy consumption metre. Data packet transmission over the WSN using the suggested DCSO-ECC technique consumes a lot less energy. The reason for this is that non-CH nodes in DCSO have the highest probability of joining benign clusters, which lowers the possibility that they will waste energy because there's a good chance their data packets will arrive at the base station on schedule. It shows that compared to the more energy-intensive current technologies, the suggested DCSO-ECC system uses less energy.

Network lifetime

The framework is regarded superior when the recommended fix lengthens network lifetime.

$$Lifetime\ \mathbb{E}[L] = \frac{\varepsilon_0 - \mathbb{E}[E_w]}{P + \lambda \mathbb{E}[E_r]} \qquad (14)$$

Where $\mathbb{E}[E_w]$ refers toproject wasted or unused energies when networks die, P implies constant continuous power consumptions of entire networks, $\varepsilon_0$refers to total non-rechargeable initial energies, λrepresents average sensor reporting rates, and $\mathbb{E}[E_r]$stands for expected reporting energies used by all sensors.

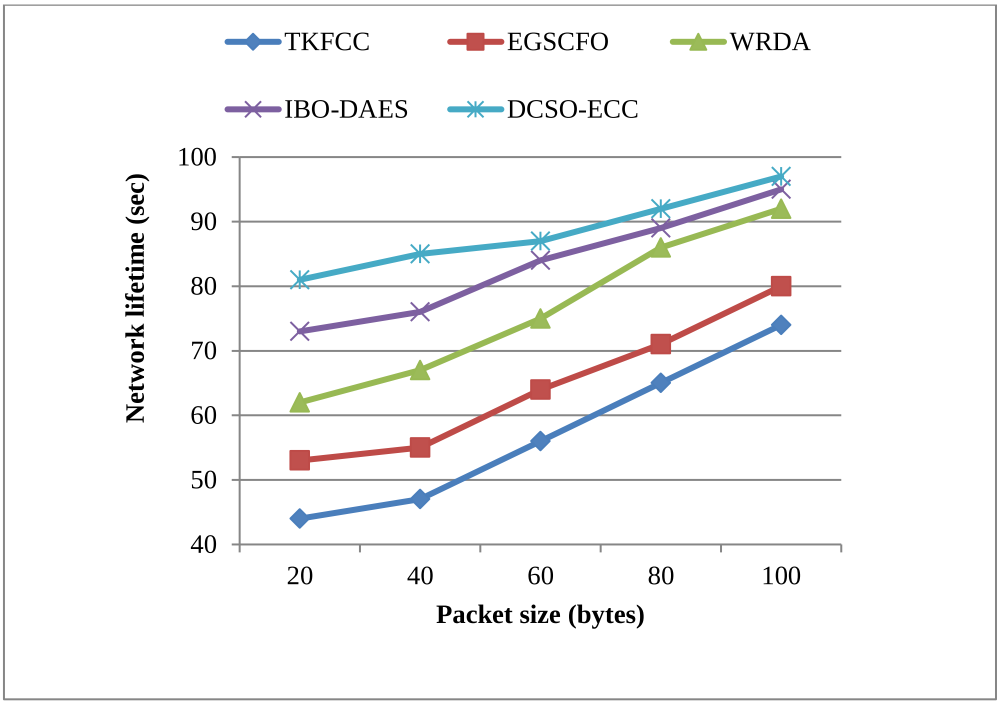

Fig 6 Network lifetime

Fig. 6 displays the network lifespan for the given packet size. The y-axis represents the network lifespan, while the x-axis represents the number of nodes. During data packet transmission, the lifespan of the sensor node is significantly extended by the proposed DCSO-ECC approach. This is because CH-based data is sent via the DCSO mechanism. Furthermore, it has been discovered that the suggested method increases the network lifespan with larger packet sizes. It illustrates that the proposed DCSO-ECC provides a longer network lifetime in comparison to the other existing WRDA, TKFCC, EGSFO, and IBO-DAES approaches.

Rate of Data Transfer

The speed at which information is sent from one location to another in a predefined amount of time is known as the data transfer rate. The speed at which a certain amount of data is sent from one location to another is known as the data transfer rate. Broadly speaking, the bandwidth of a route rises with the data transmission rate..

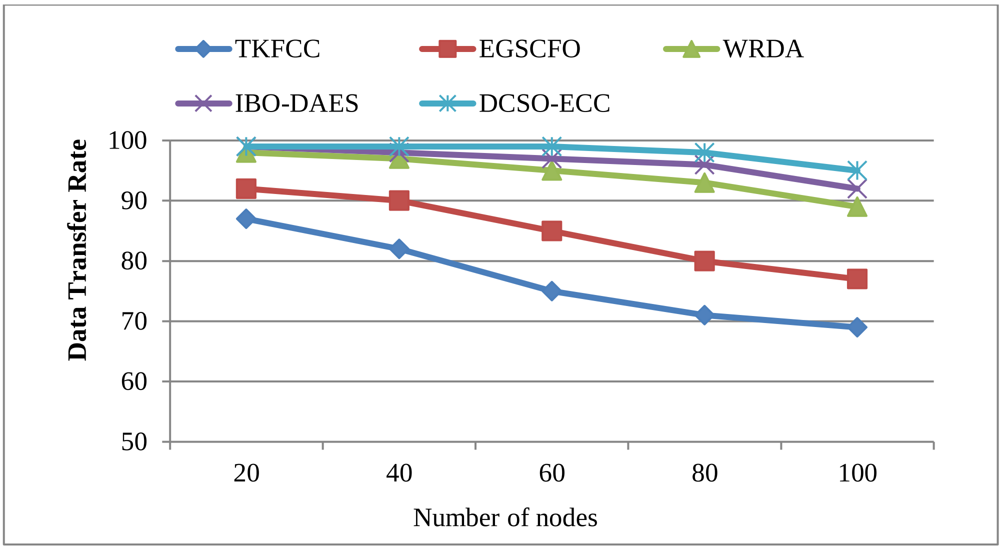

Fig 7 Data transfer rate

From the above Fig 7, it can observe that the comparison of existing TKFCC, EGSCFO, WRDA, IBO-DAES proposed DCSO-ECC algorithms in terms of data transfer rate. x axis plot the counts of nodes and in y axis the data transfer rate values are plotted. In existing scenario, the data transfer rate values are lower by using TKFCC, EGSCFO, WRDA, IBO-DAES algorithmsmethods. In proposed system, the data transfer rate value is improved significantly by using the proposed DCSO-ECC algorithm. Thus it shows that efficient and secured data transmission in WSN is performed by using proposed DCSO-ECC method

5. Conclusion

This work has suggested DCSO-ECC technique to optimize CH node selections and secure data transmissions via WSNs using IoT. Only when CS-based clustering is handled with appropriate CH selection combined with CS-based data gathering does the IoT-based WSN obtain the best network efficiency. The suggested method enhances routing performance while also choosing CH in an energy-efficient manner. The data is routed among nodes or to the sink, which improves CH selection. DCSO techniqueis used toselectbest CH nodes through fitness values. The fitness function, along with the remaining energy, throughput, and total delay, are all factors that must be considered while selecting a CH node to accomplish the optimal outcome. The DSR protocol is designed to enhance the efficiency of IoT-based WSNs by enhancing secured multipath routes for data transmissions employing functions for route discoveries and managements. The ECC method is employed to enhance secured data transfer, whereas the DSR and ECC strategy concentrate on handling fault tolerance. According to the findings, the suggested DCSO-ECC solution has a greater throughput, data transfer rate, longer network lifetime, and uses less energy than the present technique. In future, Compressive Sensing (CS) can be proposed for theenhancement of IoT based WSN performance to better packet loss ratio, delay and network’s remaining energy

References

[1] Haseeb, Khalid, et al. "An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN." *Energies* 12.21 (2019): 4174.

[2] Li, Xiong, et al. "A robust and energy efficient authentication protocol for industrial internet of things." *IEEE Internet of Things Journal* 5.3 (2017): 1606-1615.

[3] Sharma, Nonita, and Ajay K. Sharma. "Cost analysis of hybrid adaptive routing protocol for heterogeneous wireless sensor network." *Sādhanā* 41 (2016): 283-288.

[4] Batra, Payal Khurana, and Krishna Kant. "LEACH-MAC: a new cluster head selection algorithm for Wireless Sensor Networks." *Wireless Networks* 22 (2016): 49-60.

[5] Khalil, Enan A., and Suat Ozdemir. "Reliable and energy efficient topology control in probabilistic wireless sensor networks via multi-objective optimization." *The Journal of Supercomputing* 73 (2017): 2632-2656.

[6] Jaiswal, Kavita, and Veena Anand. "An optimal QoS-aware multipath routing protocol for IoT based wireless sensor networks." *2019 3rd international conference on electronics, communication and aerospace technology (ICECA)*. IEEE, 2019.

[7] John, Aniji, Angaha Rajput, and K. Vinoth Babu. "Energy saving cluster head selection in wireless sensor networks for internet of things applications." *2017 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2017.

[8] Wang, Zijing, Xiaoqi Qin, and Baoling Liu. "An energy-efficient clustering routing algorithm for WSN-assisted IoT." *2018 IEEE wireless communications and networking conference (WCNC)*. IEEE, 2018.

[9] Rani, Shalli, et al. "A novel scheme for an energy efficient Internet of Things based on wireless sensor networks." *Sensors* 15.11 (2015): 28603-28626.

[10] Mahajan, Shilpa, Jyoteesh Malhotra, and Sandeep Sharma. "An energy balanced QoS based cluster head selection strategy for WSN." *Egyptian Informatics Journal* 15.3 (2014): 189-199

[11] Saidi, Ahmed, Khelifa Benahmed, and Nouredine Seddiki. "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks." *Ad Hoc Networks* 106 (2020): 102215

[12] Agarkhed, Jayashree, Patil Yogita Dattatraya, and Siddrama Patil. "Multi-QoS constraint multipath routing in cluster-based wireless sensor network." *International Journal of Information Technology* 13.3 (2021): 865-876.

[13] Chan, Wai Hong Ronald, et al. "Adaptive duty cycling in sensor networks with energy harvesting using continuous-time Markov chain and fluid models." *IEEE Journal on Selected Areas in Communications* 33.12 (2015): 2687-2700

[14] Ahmed, Khaled, Aboul Ella Hassanien, and Siddhartha Bhattacharyya. "A novel chaotic chicken swarm optimization algorithm for feature selection." *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*. IEEE, 2017.

[15] Wu, Dinghui, Shipeng Xu, and Fei Kong. "Convergence analysis and improvement of the chicken swarm optimization algorithm." *IEEE Access* 4 (2016): 9400-9412

[16] Bolla, Dileep Reddy, et al. "Energy-efficient dynamic source routing in wireless sensor networks." *Emerging Research in Computing, Information, Communication and Applications: Proceedings of ERCICA 2022*. Singapore: Springer Nature Singapore, 2022. 749-763.

[17] Abdullah, Md, Mohammad Muntasir Rahman, and Mukul Chandra Roy. "Detecting sinkhole attacks in wireless sensor network using hop count." *International Journal of Computer Network and Information Security* 7.3 (2015): 50-56.

[18] Boahen, Edward Kwadwo, James Ben Hayfron-Acquah, and Frimpong Twum. "An enhanced elliptic curve cryptosystem for securing data." *International Journal of Computer Applications* 182.9 (2018): 47-53

[19] Yang, Liu, et al. "An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks." *IEEE Sensors Journal* 21.12 (2021): 13935-13947.

[20] Augustine, Susan, and John Patrick Ananth. "Taylor kernel fuzzy C-means clustering algorithm for trust and energy-aware cluster head selection in wireless sensor networks." *Wireless Networks* 26 (2020): 5113-5132