International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223311 Volume 10, Issue 4, July – August (2023)

RESEARCH ARTICLE

Empowered Chicken Swarm Optimization with Intuitionistic Fuzzy Trust Model for Optimized Secure and Energy Aware Data Transmission in Clustered Wireless Sensor Networks

A. Anitha
Department of Computer Science, Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India.
anithaaruchamy91@gmail.com

S. Mythili
Department of Information Technology, Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India.
smythili78@gmail.com

Received: 09 May 2023 / Revised: 29 June 2023 / Accepted: 14 July 2023 / Published: 31 August 2023

Abstract – Each sensor node functions autonomously to conduct data transmission in wireless sensor networks. It is very essential to focus on energy dissipation and sensor nodes lifespan. There are many existing energy consumption models, and the problem of selecting optimized cluster head along with efficient path selection is still challenging. To address this energy consumption issue in an effective way the proposed work is designed with a two-phase model for performing cluster head selection, clustering, and optimized route selection for the secure transmission of data packets with reduced overhead. The scope of the proposed methodology is to choose the most prominent cluster head and assistant cluster head which aids in prolonging the network lifespan and also securing the inter-cluster components from selective forwarding attack (SFA) and black hole attack (BHA). The proposed methodology is Empowered Chicken Swarm Optimization (ECSO) with Intuitionistic Fuzzy Trust Model (IFTM) in Inter-Cluster communication. ECSO provides an efficient clustering technique and cluster head selection and IFTM provides a secure and fast routing path from SFA and BHA for Inter-Cluster Single-Hop and Multi-Hop Communication. ESCO uses chaos theory for local optima in cluster head selection. The IFTM incorporates reliance of neighbourhood nodes, derived confidence of nodes, estimation of data propagation of nodes and an element of trustworthiness of nodes are used to implement security in inter-cluster communication. Experimental results prove that the proposed methodology outperforms the existing approaches by increasing packet delivery ratio and throughput, and minimizing packet drop ratio and energy consumption.

Index Terms – Wireless Sensor Networks, Chicken Swarm Optimization, Intuitionistic Fuzzy Trust Model, Energy Aware, Security, Cluster Head, Clustering and Inter-Cluster Communication.

1. INTRODUCTION

Resources like energy, computing power, storage, and transmission range are only a few limitations that define wireless sensor networks (WSNs) [1]. Out of these elements, the wireless sensor networks' main resource restriction has been the energy of sensors. In ad-hoc networks like WSNs, a structural organization is recognized as a practical model to assure stable, trustworthy, reliable, and efficient infrastructures. Wireless sensor network has the following merits scalability, high flexibility, and capability to use in various environments leading a pathway to the usage of the technology in numerous sectors [2].

One of the methods used most frequently for managing WSN topology is clustering. A clustering explores positions nodes into a collection of groupings known as clusters according to a set of predetermined requirements like ensuring QoS, minimizing consumption of resources, and network traffic [3]. Every cluster consists of Cluster Heads (CHs), which collects information from cluster members to decide whether to transfer the packets directly to BS or indirectly by utilizing intermediary nodes [4]. By using clustering strategies, resource-limited nodes can avoid sending their data requests directly to gateway nodes upshots in energy surplus, inefficient resource use, and intrusion. Sensor nodes involved in data collection and transmission processes are predisposed to attacks [5]. The prevalent downside of WSN is sensor nodes energy is highly restricted and network resources are inadequate [6].

RESEARCH ARTICLE

The WSN clustering protocol allows for communication to take place either intra-cluster, or between the clusters and the BS, or inter-cluster, or between the clusters [7]. Selective information loss or not sending sensitive information is a frequent assault that disrupts the regular transfer of network data. Network layer attacks known as Selective Forwarding Attacks (SFA) [7] are common in WSNs. In this network, the data packets generated by the source nodes are forwarded to their closest sensor nodes to attempt to maintain the belief aspects. From there, they forward packets of data to their target. In the additional, certain SFAs are designed to allow the intruders' sensor nodes to be designed to pretend as authentic sensor nodes. Following that, these attacking nodes will rapidly eliminate the data packets that were recently acquired and only send selected packets of data to closest node. The malicious sensor nodes discard whole packets of data received rather than passing them along to the surrounding nodes. This type of assault is referred to as a "black hole attack." [8].

1.1. Problem Statement

Wireless clustering protocol allows for communication to take place either intra-cluster, that is, within the clusters, or inter-cluster, that is, between the clusters and the BS. When the propagation delay exponent is substantial multi-hop interaction between node sensors and the cluster head is more economical than single-hop communication. Signal propagation problems can be effectively resolved in such situations through multi-hop communication. However, the radio signal starts to dissipate. Security in sensor networks presents a significant problem since it must strike a balance between resource conservation and security maximization. The limitations of the sensor node affect its privacy. A node could be targeted mainly by internal attacks namely SFA and BHA which is launched upon CWSN, making it vulnerable to leaking private information and acting like another node. And selecting the most energy-efficient cluster head is also a tedious process. Hence, the existing methodologies have a limitation of missing in securing each state of clustering nodes in inter-cluster communication such as cluster head, cluster member, transient node, and gateway node also it does not focus effectively on energy consumption. So it needs to be protected against encountering those attacks by providing energy-aware routing Thus, the proposed work ECSO + IFTM develops to address this by imposing a secure and energy-aware routing in inter-cluster communication along with effective discovery, avoidance and rescuing mechanism from SFA and BHA.

1.2. Research Objectives

The proposed methodology is implemented to perform the detection, prevention, and recovery mechanism of cluster head node, cluster member node, transient node as well as gateway node from SFA and BHA in inter-cluster communication.

The main contributions of the proposed work are as follows:

- To aim at minimal energy consumption with a secure and prolonged lifetime.
- To meet the need for minimal energy consumption with a high level of safety.
- Empowered chicken swarm optimization algorithm used for potential cluster head selection and uncertainty-based route selection using an intuitionistic fuzzy trust model.
- The proposed model handles precisely both SFA and BHA.
- Cluster head, cluster member, transient member, and gateway node are protected in inter-cluster communication.
- Assistant cluster head is carefully chosen to manage and persist through the network operation, even if the cluster head meets any issue.
- Ensures providing secure and energy-aware routing in inter-cluster communication.
- Maximizes packet delivery percentage and throughput, minimizes energy depletion, and packet loss rate in order to improve the network efficiency and lifetime.

1.3. Organization of the Paper

The Section 2 discusses the literature review in relation to the problem statement. Section 3 describes in detail about the work of the proposed approach ECSO + IFTM. Section 4 presents the experimental data and includes a discussion of the performance metrics-based comparative analysis. Finally, Section 5 accomplishes by demonstrating the effectiveness of the suggested technique in achieving the targeted objectives of the research.

2. LITERATURE REVIEW

El Khediri et al. [9] proposed a “Multiple Weight-Low Energy Adaptive Clustering Hierarchy” (MW-LEACH) algorithm used in selection of cluster head based on excess energy in the region around the density's center. By moving in various directions and sending that specific data to the BS, these candidates gather information from their members in greater depth. This methodology is quick, guarantees adequate fault tolerance levels, and has fewer message and time issues. It limits concentrating on other cluster components and in the homogeneous network sensor nodes have only restricted energy.

Hicham Qabouche et al. [10] proposed a protocol called “Reliable and Dynamic with Energy Aware Routing”

RESEARCH ARTICLE

(RDEAR) protocol which is used for minimizing energy dissipation and enhancing credibility via nodes of respective cluster as their relay nodes in intra cluster communication. The inter cluster communication is performed using gateway selection in terms of density, transmission range and energy of the cluster heads. It aids in routing maintenance of cluster heads with minimal energy consumption, provides many reliable links, and fights data loss. There is a lack in handling the routing issue, and security is less while considering all the cluster components.

Srinivasa Rao Et al. [11] proposed a "Spatial-Temporal Fuzzy Inference System" (SRFIS) approach (i.e.) used for safeguarding network against outliers, which aids in security by identifying outliers before allowing data transfer. The weight values pertaining to the factors affecting safety and proximity value are examined during optimization. The Euclidean distance amongst nodes that communicate is determined, and a set of fuzzy inference guidelines is developed to detect outliers based on distance, energy, and mobility characteristics. The best routing pathways can be identified by calculating the best fitness function with a combined Crow-Whale Optimisation strategy. It is implemented to ensure that communication across source and destination endpoints is reliable. Security is moderate and requires an additional approach from trustable and secure data transmission.

Mehetre et al. [12] proposed a "two-stage security mechanism and dual assurance scheme." The two-state security mechanism is used for node selection by detecting the nodes with detection packets and trust. The dual assurance scheme is a dependable and trustworthy routing technique providing packet validation and security. This scheme is used to choose the trustable nodes and protect the data stream. To defend against various routing attacks these solutions rely on pre-emptive trust. This work finds a reliable route by combining confidence with the meta-heuristic cuckoo search strategy. It limits the number of sensor nodes and does not suit large-scale networks.

Yadav and Mahapatra [13] proposed "Cuckoo Insisted-Rider Optimization" (CI-ROA) designed for choosing the cluster head and also routing. And it is a grouping of the cuckoo search algorithm and rider optimization algorithm. This methodology aims at the metrics like energy, distance, and delay. It does not concentrate on secure data transmission and lacks in focusing on the other cluster components.

Mehbodniya et al. [14] presented "Energy-Aware Proportional Fairness Multi-User Routing" (EPFMR) helps in energy consumption ratio. The "Greedy Instance Fair Method" (GIFM) is used to quantify energy on multi-user route paths developed for packet flow. In EPFMR, the GIFM creates node reliant on dynamism of operative confined pathways by increasing throughput. The Boltzmann Distribution (BD) is used to lower Route Searching Time (RST) and energy on multi-consumer wireless sensor network is minimized. The presented routing employs request period difference performs path analysis to achieve minimal energy consumption. The time spent is costly and requires extra effort.

Vinodhini et al. [15] proposed an integration of two strategies. First strategy is fuzzy logic which is used to perform unequal clustering and the second strategy is the optimization algorithms which performs the process of routing. In this, the radius of clusters will be unequal and overcrowded regions comprised of smaller radius and it promotes network traffic and depletion of network energy. Once the cluster formation is over," Glow worm Swarm Optimization" (GSO) procedure performs routing path selection based on the data framework to perform data transmission. It may sometimes cause an increase in energy consumption and time.

Udhayavani et al. [16] suggested a trust aware routing framework (TARF) for providing security in WSN. It is an adaptive intermittent threshold delicate energy proficient network procedure. It aids in improved quality of service with an additional reliable and energy-efficient approach by lessening attacks and increasing the network lifetime. It emphasizes trust-aware routing but not the clustering process and cluster head selection. Table 1 gives a brief outline about the research methodologies discussed.

Table 1 Summarization of Related Works

Reference	Findings	Limitations
El Khediri et al. [9]	Residual energy of sensor node is taken into consideration to perform cluster head election. The sensor nodes can collect data from various directions.	It concentrates only on cluster head selection but not on the other cluster components like intermediary nodes and cluster member nodes. All nodes have restricted energy.
Hicham Qabouche et al. [10]	The node belonging to the same cluster uses its relay nodes in the intra-cluster, whereas	There is a lack in handling the routing issue, and security is less while

RESEARCH ARTICLE

	gateway selection needs to be performed to establish an inter-cluster communication.	considering all the cluster components.
Srinivasa Rao et al. [11]	Identifying the outliers before data transmission. The optimal fitness function is used for routing.	Security is moderate and requires an additional approach for trustable data transmission.
Mehetre et al. [12]	Safe routing paths are used based on node selection and trust.	Suitable for minimal number of nodes and not adaptable for large-scale networks.
Yadav et al. [13]	Optimization techniques for routing	It does not concentrate on secure data transmission and other cluster components.
Mehbodniya et al. [14]	Packet flow carried out based on relationship between request periods of sensor nodes and also computes multi-user routing path.	It requires extra time and effort.
Vinodhini et al. [15]	Overcrowded areas contain smaller radius aids in load balancing and energy consumption. Data routes are selected based on the data context.	Sometimes this may lead to the depletion of network resources and energy depletion.
Udhayavani et al. [16]	An energy efficiency trust aware routing protocol.	It does not focus on clustering and cluster head selection.

3. PROPOSED METHODOLOGY

Single routing protocol does not work effectively in various applications. So, multi-hop routing is the most prominent step among the sensor networks in different network architectures resulting in minimal energy consumption. Clustering is the process which aids in prolonging network lifespan by providing prodigious network performance. Clustering and data aggregation are the other vital techniques that incorporate effective data communication and minimal energy consumption. There are two forms of inter cluster communication depicted in Figure 1.

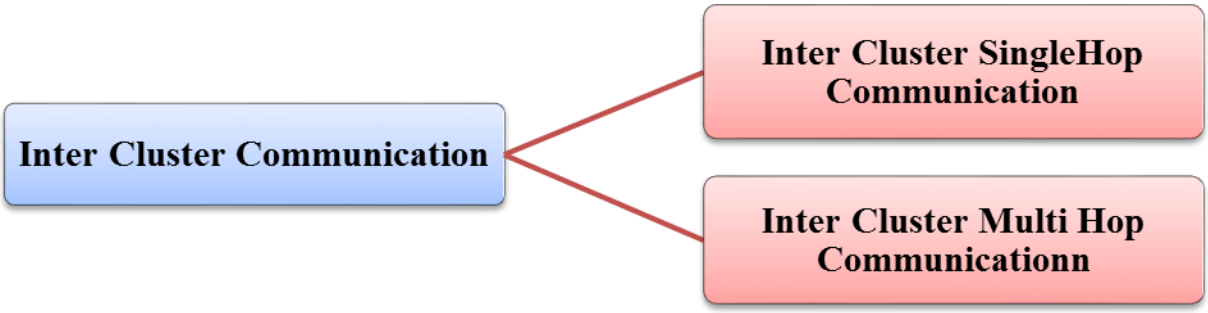

Figure 1 Two forms of Inter Cluster Communication

3.1. Inter-Cluster Single-Hop Communication

Figure 2 Inter Cluster Single-Hop Communication

It is applicable when the cluster heads CHs) are in a specified range to reach the base station (BS) and can establish a direct connection (i.e.) from CHs to BS and vice versa for successful data transmission. This form of cluster communication occurs between the CHs and BS, where all the cluster members of the cluster will send data packets to its respective CHs. Then CHs aggregates the requested data of all its CMs. Once the data aggregation is performed, CHs will forward that aggregated data to its BS. And the inter-cluster single-hop communication is represented in Figure 2.

3.2. Inter-Cluster Multi-Hop Communication

It is defined as indirect communication which is established based on the reachability of the cluster heads to its base station. When the CMs want to communicate with its CH but it is farther from the CMs then an intermediate node called transient nodes (TNs) establishes the connection between its CMs and CHs to perform cluster communication. In multi-hop communication, the location of the BS is calculated, and based on the multi-hop routing takes. Sometimes CHs can directly communicate with the BS (i.e.) from CMs to TNs to CHs and BS and vice versa. Likewise, when BS distance is farther from CHs then the communication takes place between CHs (i.e.) CMs to TNs to CHs to CHs to BS, and

RESEARCH ARTICLE

also it chooses the other way in multi-hops (i.e.) CMs to TNs to CHs to GWs to CHs to BS and vice versa. And the inter cluster multi-hop communication is presented in Figure 3.

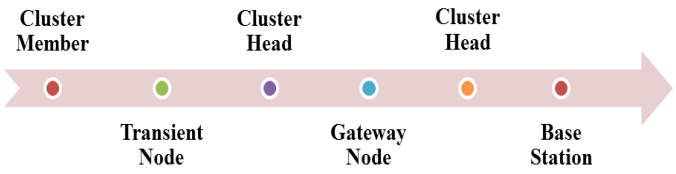

Figure 3 Inter-Cluster Multi-Hop Communication

The proposed methodology "Empowered Chicken Swarm Optimization with Intuitionistic Fuzzy Based Trust Model (ESCO +IFTM)" is developed for the Detection, Prevention, and Recovery of Cluster Head, Cluster Member, Intermediary Nodes, and Gateway Nodes from Selective Forwarding Attack (SFA) and Black Hole Attack (BHA). It focuses on providing secure and energy-aware inter-cluster single-hop and multi-hop communications. It also focuses on each component of inter-cluster sensor nodes such as cluster members, cluster heads, intermediary nodes, and gateway nodes from SFA and BHA.

"ESCO +IFTM" aims to handle both restricted energy usage and secure data transmission by developing two different strategies. ESCO is used to perform energy efficient clustering and also choosing the prominent cluster head for communication and it works based on the inspiration of food foraging behaviour of chickens. Their hierarchical structure with rooster, mother hens, and chickens is used for electing the cluster heads and transient nodes for data aggregation from source nodes within a cluster.

The cluster heads are nominated depending on the capability assessment of each node is computed based on energy depletion and node density. The nodes with the best fitness value are considered cluster heads and involve in intercommunication during data transmission. The cluster heads are elected to transmit data securely. An uncertainty model is the generalization of fuzzy logic known as intuitionistic fuzzification is applied to evaluate the trust model of each transient and gateway node. The framework of the proposed Empowered Chickens swarm optimization with the Intuitionistic fuzzy-based Trust Model (ECSO+IFTM) is illustrated in Figure 4.

The main contributions of the proposed work are as follows:

- The proposed methodology focused on secure and energy-aware data communication in inter-cluster.
- Clustering and cluster head selection are made effectively by implementing ESCO algorithm. The fitness value and optimal solution is used in the selection of cluster head, assistant cluster head, gateway node, intermediary nodes, and cluster members. This helps in performing uninterrupted energy-efficient data transmission between clusters.
- IFTM strategy helps in secure and energy conscious data transmission in inter-cluster communication.
- A comparison is made with existing approaches such as MW-LEACH, TARF, and RDEAR to prove the proposed methodology works more effectively.

3.3. EMPOWERED CHICKEN SWARM OPTIMIZATION (ECSO)

The Conventional Chicken Swarm Optimisation (CSO) algorithm [17] evolves to the socially arranged behavior of farm chickens. Figure 5 depicts the scenario before implementing the proposed methodology. In the social interactions of chickens, hierarchical order is vital. In a flock, the dominant chickens will rule over the underdogs. The more subservient hens and roosters are situated towards the group's periphery, while the more leading hens prefer to stay nearby to head roosters. Social order would be temporarily upset by adding or removing hens from a flock until a clear hierarchy is formed.

A single rooster, some hens, and chicks are found in each of the many groupings that make up a chicken swarm. The rooster serves as the flock's leader in chicken farms. A rooster is chosen as the group leader in each group based on how well he can find food, and the group also consists of chicks and hens, as indicated in the image. Based on this structure, the CSO is displayed. The rooster, chicks, and mother hens are symbolized as RH, CK, and MH, respectively, when the CSO algorithm begins by running on M populations of chickens [18]. The hierarchical organization of chickens relies on their fitness value shown in Figure 6.

Each group's rooster serves as a leader and directs the movement of the chickens by adjusting their positions concerning their food source. The hens with the highest fitness score are chosen to serve as the rooster's leader, while hens with the lowest fitness scores are classified as chicks. The other fowl take on the role of the hens. Hen and chick interactions are a lot like parental relationships in that they develop randomly.

The parental link and the dominant position within a group will remain constant. During the food-finding process, the roosters (RSN) spontaneously identify their meal and consume more of it. The next best in the group are the mother hens, who supply food for both themselves and the chicks, who are their only source of protection and sustenance. The remaining food divided among the hens. Roosters are therefore given priority, next to mother hens are co-leaders, older hens are hens, and chicks are members, in order of diminishing fitness values.

RESEARCH ARTICLE

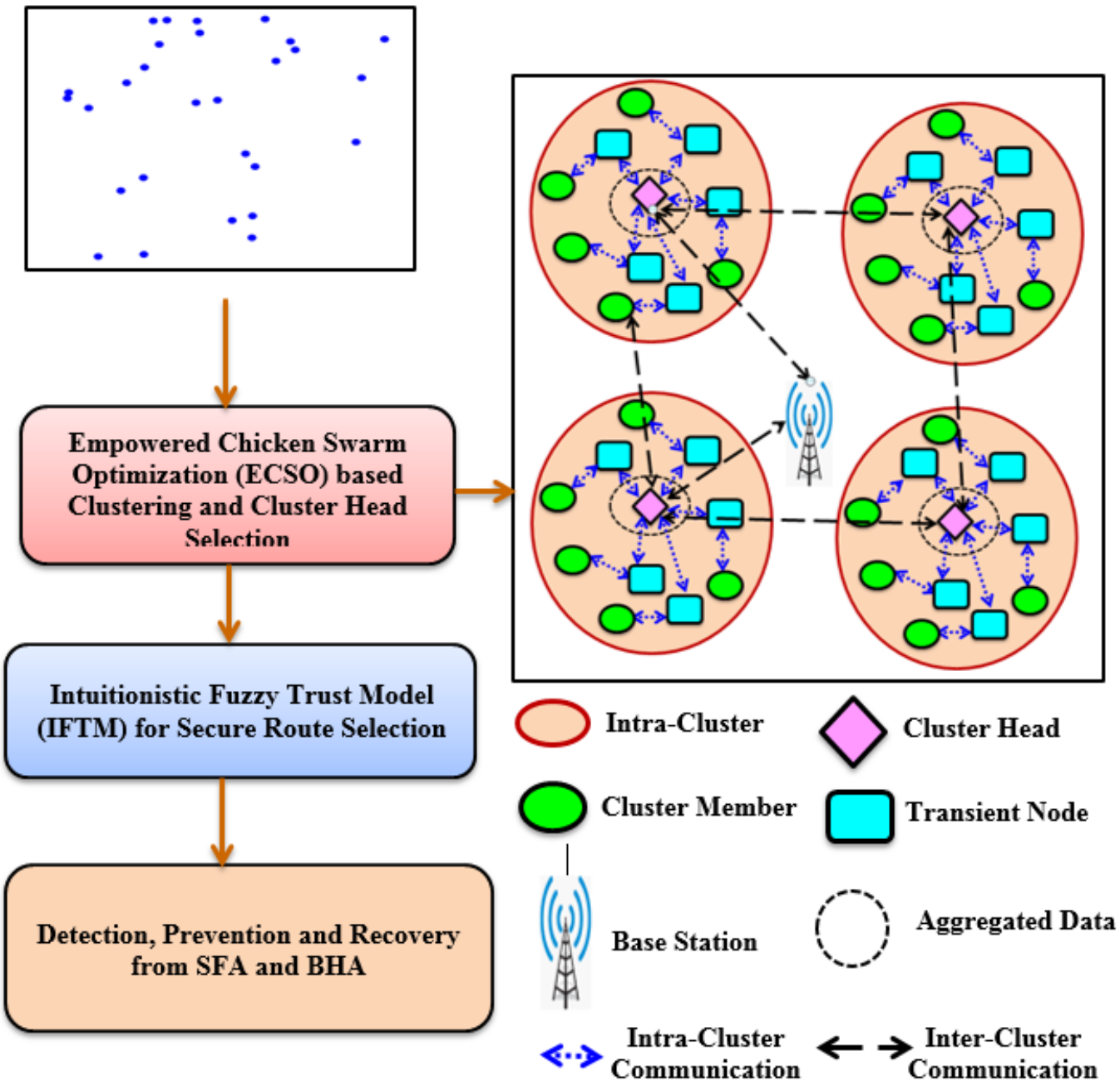

Figure 4 Overall Structural Design of Empowered Chicken Swarm Optimization with Intuitionistic Fuzzy Trust Model for Secure and Energy Aware Data Transmission in Clustered WSN

In the conventional models, the cluster heads are selected arbitrarily, and the clusters are constructed on their node consistency and enduring energy. Again, re-clustering is done based on applying using Euclidean distance.

3.3.1. Behaviour of Chicken Swarm

The roosters with the highest fitness values receive preference over those with lower fitness values when it comes to acquiring food [19]. Chaos mapping is used for the movement of chickens to overcome the limitation of local search optima performed randomly.

While roosters with lower fitness values have substantially less space for hunting, those with greater fitness ratings can locate food in a wider range of areas. And it is described by the equation (1) and (2).

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223311 Volume 10, Issue 4, July – August (2023)

RESEARCH ARTICLE

$$P_{i,j}^{t+1} = P_{i,j}^{t} * (1 + \mathrm{C}(0, \beta^2)) \quad (1)$$

$$\beta^2 = \begin{cases} 1, & if\ ft_i \le ft_m, \\ Ep\left(\frac{ft_m - ft_j}{|ft_j| + \nu}\right), & else, m\ \epsilon [1, T], m \ne j \end{cases} \quad (2)$$

With 0 as its mean value, the Gaussian probability $\mathrm{C}(0, \beta^2)$ is represented by the notation C (0, 2). The symbol for the standard deviation is β. To avoid zero division, a second smallest constant, "'ν'" is added. The score of a rooster, m, is chosen at random among a set of roosters, while ft denotes the fitness value based on 'p'. Hens in a group follow the roosters in pursuit of food. They arbitrarily pick up feed from other groups of chickens. In the feeding competition, the more aggressive hens prevailed against the subservient birds.

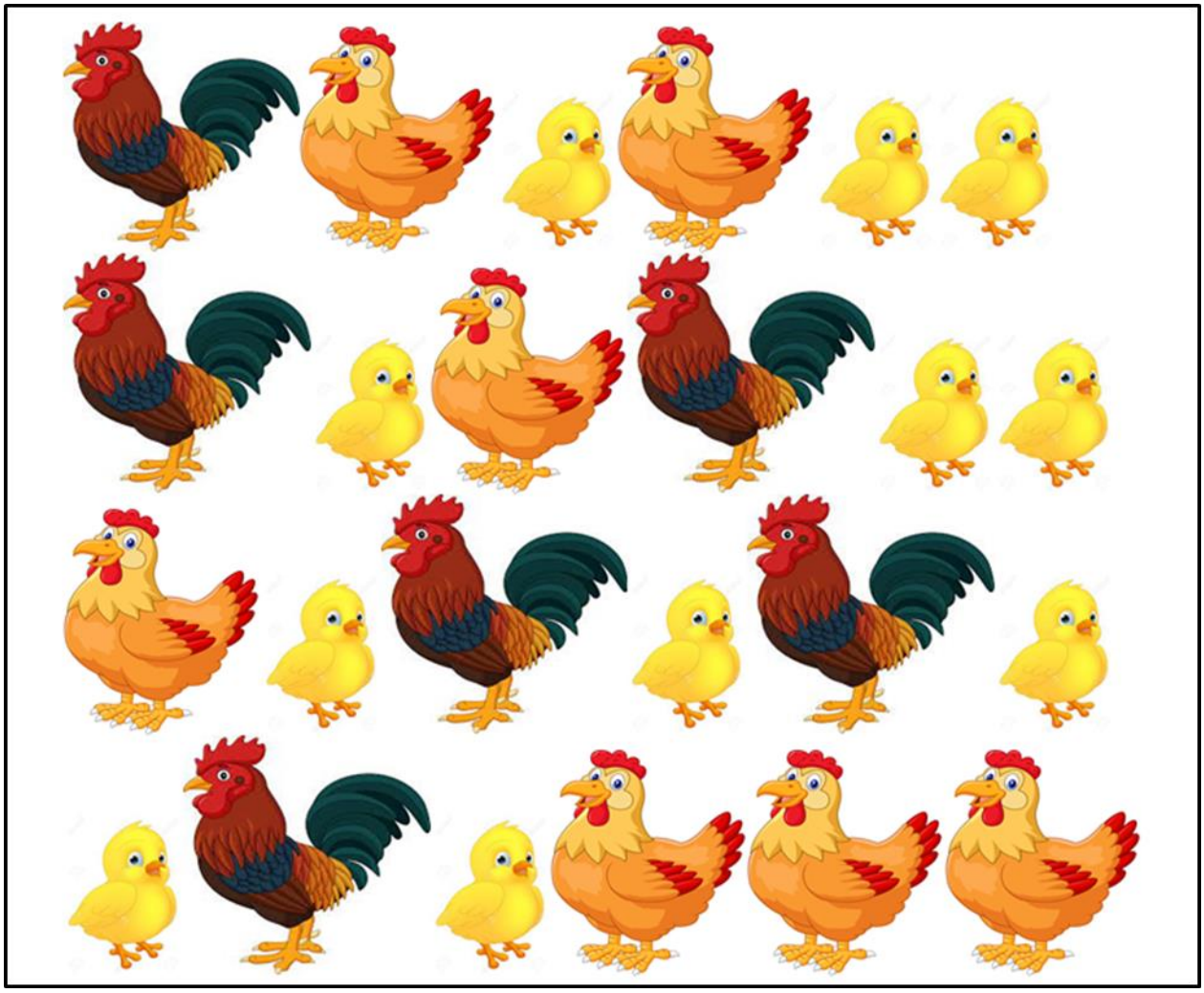

Figure 5 Chicken Swarm before Implementing ECSO + IFTM

Equations (3) to (7) are used for describing the connection between the behaviour and motion of chickens is displayed. To frame the hierarchy of nodes in every cluster, the nodes forward data packets with their fitness value is evaluated using their initial and residual energy. The ft denotes the fitness value evaluation as formulated.

$$ft = \begin{cases} 0.8 * \frac{\varepsilon_{rs}}{\varepsilon_{it}} + 0.2 * \frac{dt_{mx} - dt}{dt_{mx} - dt_{min}}, if \varepsilon_{rs} < 0 \\ 0.2 * \frac{\varepsilon_{rs}}{\varepsilon_{it}} + 0.8 * \frac{dt_{mx} - dt}{dt_{mx} - dt_{min}}, if \varepsilon_{rs} \ge 0 \end{cases} \quad (3)$$

$$p_{i,j}^{t+1} = p_{i,j}^{t} + u1 * rn * \left(p_{rh1,j}^{t} = p_{i,j}^{t}\right) + u2 * \mathrm{C} * (p_{rh2,j}^{t} = p_{i,j}^{t}) \quad (4)$$

$$p_{i,j}^{t+1} = p_{i,j}^{t} + u1 * rn * \left(p_{rh1,j}^{t} = p_{i,j}^{t}\right) + u2 * \mathrm{C} * (p_{rh2,j}^{t} = p_{i,j}^{t}) \quad (5)$$

$$u1 = \mathrm{Ep}((ft_i - ft_{rh1})/(abs(ft_i) + \gamma)) \quad (6)$$

$$u2 = \mathrm{Ep}((ft_{rh2} - ft_i)) \quad (7)$$

Where C is a uniform random number with value ranging from 0 to 1. The rooster from i^{th} hen group index is

RESEARCH ARTICLE

represented as rh1 ∈[1, …, M]. Either hen or rooster chicken index chosen arbitrarily form the flock is rh2 ∈[1, …, M] with the condition rh1 ≠ rh2.

Discernibly, $ft_i > ft_{rh1}, ft_i > ft_{rh2}$, thus $u2 < 1 < u1$. If u1=0. The group's other chickens will follow the ith hen in starting to search for food. The smaller u2 result in the widest gap between the positions of the two hens when there is a significant difference in fitness levels between them which helps to prevent hens from stealing food from other chickens. This is because the rooster and the chickens' fitness values are viewed as competition by the other chickens in the group.

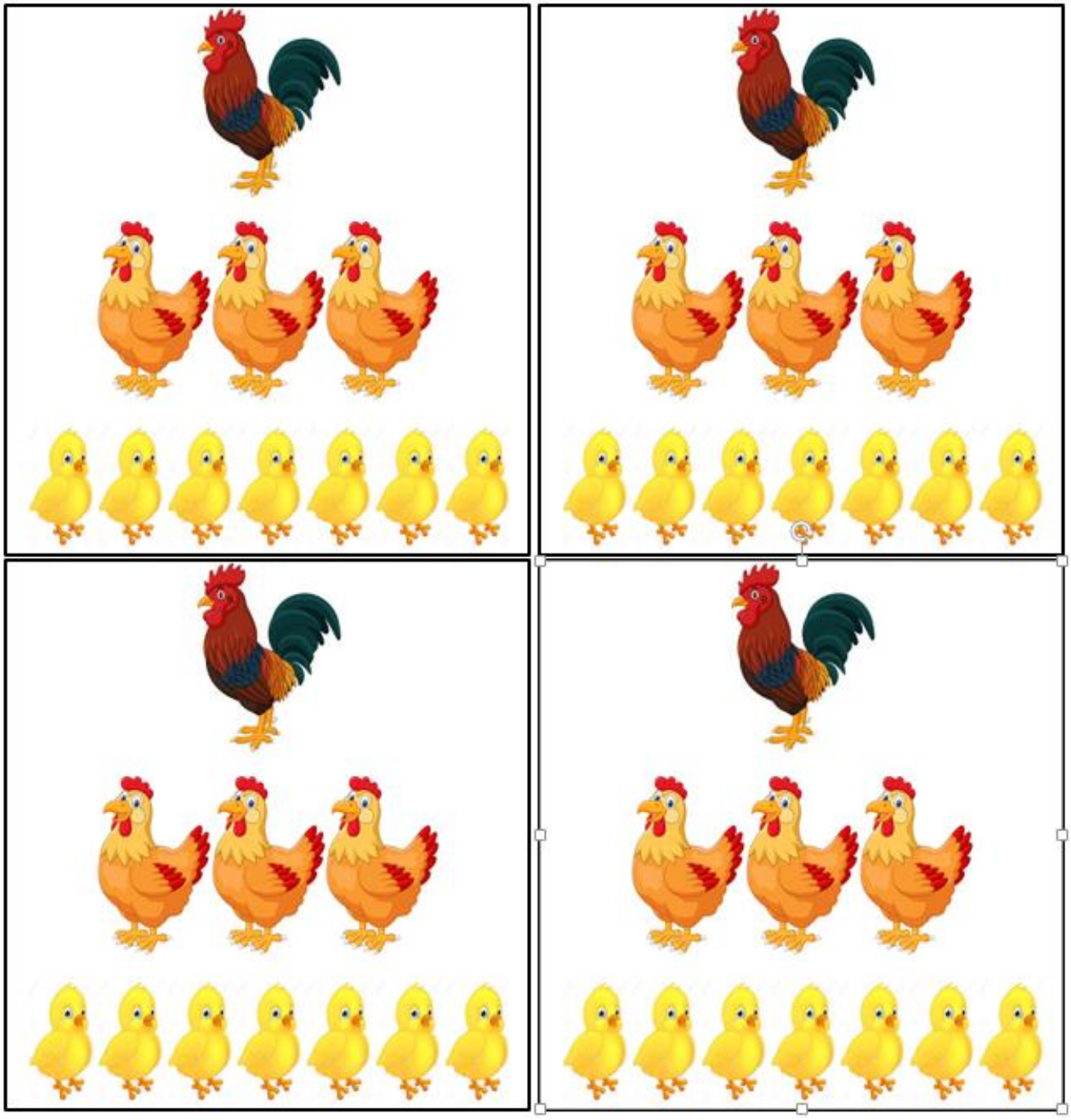

Figure 6 Chicken groups Hierarchical Organization after Implementing ECSO + IFTM

RESEARCH ARTICLE

Equation (8) illustrates how the chicks seek food while moving around their mother hen.

$$p_{i,j}^{t+1} = p_{i,j}^{t} + CK * (p_{m,j}^{t} - p_{i,j}^{t}) \quad (8)$$

Where $p_{m,j}^{t}$ indicates the i[th] chick's mother location, CK represents a chick pursuing its mother's food foraging. Additionally, the hens' placement in this case is picked randomly, which could cause early convergence. An enhanced location to look for food is used to get around this erroneously chaotic mapping process. The chaotic function used to update the position of the rooster / Cluster head is selected as a leader, as illustrated in equation (9).

$$s_{i,j}^{p+1} = s_{i,j}^{p} \times (1 + \theta_{i,j} \times rnd(0, \gamma^2)) \quad (9)$$

The location of co-leaders / intermediary nodes and elders are modified as given in the equation (10)

$$s_{i,j}^{p+1} = s_{i,j}^{p} + u1 \times \theta_{i,j} \times \left(s_{rh1,j}^{p} - s_{i,j}^{p}\right) + u2 \times \theta_{i,j} \times (s_{rh2,j}^{p} - s_{i,j}^{p}) \quad (10)$$

As per equation (11) the location of remaining members within cluster nodes in the group are formulated.

$$s_{i,j}^{p+1} = s_{i,j}^{p} + CK \times \theta_{i,j} \times (s_{m,j}^{p} - s_{i,j}^{p}) \quad (11)$$

3.3.2. Performing Clustering and Cluster Head Election using ECSO

Most of the prevailing clustering models generally communicate packets of data to base station or destination directly which results in energy depletion and a high possibility of packet dropping ratio. To overcome the existing data transmission overhead issue, hence this proposed methodology is introduced with a novel inter-cluster communication among cluster heads with the highest trust values. The cluster head is responsible in forwarding data requests of its cluster member by data aggregation process it leads the accumulated data requests to its nearby sink node. The data response in association with the received data requests is generated then it will be forward to its intended recipient; each rooster is used as the gateway for performing secured intercommunication in WSN. The discovery of the best secure path is achieved by an intuitionistic fuzzy trust model, which computes the genuineness of each forwarding gateway node (rooster of other clusters) along with their distance towards the sink node.

Algorithm 1 states the ECSO for clustering and cluster head selection in WSN. At first, all sensor nodes are positioned within deployment area. After deployment process, fitness value is calculated for each and every sensor nodes. The finest solution is derived by assigning weightage to each sensor nodes. The hierarchical order is formed based on the fitness value of nodes. The rooster which gets the uppermost fitness value will get elected as cluster head and hens with highest fitness value will be considered to be assistant cluster head. The nodes with the second fitness value are considered to be transient nodes. Whenever there is a necessity the rooster will act as the gateway node which acts as the bridge between two or more clusters to perform inter-cluster communication.

Equations (9) to (11) are used to discover optimum value for updating the position of chicken swarm. Equation (9) is used for updating the position of rooster head (i.e.) cluster head also at times as gateway node. Equation (10) is used for updating the position of co-leader (i.e.) intermediary nodes which act as assistant cluster head and transient nodes of each cluster. And equation (11) is used to update the position of chicks (i.e.) cluster members of each cluster. Then the new solution is calculated to determine the nodes with the highest energy and this helps in electing the hens or chicks with maximum energy as cluster head. Based on new solution the hens or chicks with maximum fitness value will be elected as new cluster head to enhance the energy depletion.

Step 1: Begin

Step 2: Initialize S as inhabitants of Sensor Nodes and other parameters

Step 3: Compute fitness value of S chicken (nodes), p=0;

Step 4: While (p < MG)

If (p % M*G* == 0)

Weight values of nodes are assigned

Evaluate and move them to the finest solution

Depending on the fitness value of each nodes sort them in hierarchical order

Cluster the nodes with their nearest highly fittest value rooster as cluster head and hens as assistant cluster head.

The transient nodes are chosen which have the second fittest value for intra-communication within the group.

End if

// To overcome local optima chaos mapping is applied

For *k* = 1 : *S*

If k == position of the leader-Rooster has been updated

$$s_{i,j}^{p+1} = s_{i,j}^{p} \times (1 + \theta_{i,j} \times rnd(0, \gamma^2))$$

If k == position of co-leader hen has been updated

$$s_{i,j}^{p+1} = s_{i,j}^{p} + u1 \times \theta_{i,j} \times \left(s_{rh1,j}^{p} - s_{i,j}^{p}\right) + u2 \times \theta_{i,j} \times (s_{rh2,j}^{p} - s_{i,j}^{p}))$$

If k == chick its position is reformed

RESEARCH ARTICLE

$s_{i,j}^{p+1} = s_{i,j}^{p} + CK \times \theta_{i,j} \times \left(s_{m,j}^{p} - s_{i,j}^{p}\right)$

End for

New solution is computed to determine the nodes with highest energy and node density as cluster head

Update the cluster member with highest fitness value as the present cluster head to improve energy depletion

End while

Step 5: End

Algorithm 1 ECSO Algorithm

3.4. Determining Secure Routing Using Intuitionistic Fuzzy Trust Model (IFTM) for Optimized Data Transmission in Clustered WSN

The fuzzy concept is used to do the necessary adjustment of parameters of the CSO algorithm. It aims on intuitive reflection about influence of parameters in association with the knowledge of human for attaining accuracy and also to enhance the algorithm [20]. Intuitionistic Fuzzification is the generalized concept of fuzzy [21, 22], the major advantage is that it not only computes "Membership Degree," but independent "Non-Membership Degree and Hesitation Degree" is also considered as a major factor to represent each real-time factor, in this case, each node transmission characteristics is represented in the triplet factor as in equation (12).

$$\text{IFS} = <\mu_c(N), \vartheta_c(N), \pi_c(N)> \quad (12)$$

The values of μ, ϑ, π lies between (0,1) [23]. The characteristic of node N is defined using intuitionistic fuzzification using the grade of membership is $\mu_c(N)$, the grade of non-membership degree is $\vartheta_c(N)$ and degree of hesitancy is $\pi_c(N)$. Defining the characteristic of nodes with hesitancy as an important factor greatly handles the problem of both selective forwarding attack and black hole attack detection more accurately.

3.4.1. Reliance of Neighbourhood Nodes

It displays the level of trust that an agent determines based on acquaintance when engaging with the target agent as given in the equation (13).

$$(L^d)_x^v(h, h+1) = S_x^z(h, h+1) \quad (13)$$

Where $(L^d)_x^z$ signifies the local trust for x[th] transaction and time interval is represented as v[th], h denotes the assessment hop and h+1 defines the hop to be assessed.

3.4.2. Derived Confidence of Nodes

Using the expertise that additional hops have amassed, derived confidence of nodes is calculated. Each hop makes use of the information from earlier hops to choose the best options to establish data transmission. On the way to build informal confidence every hop asks its other hops for opinions. Final hop compiles suggestions from other hops and input about the reliability of the suggested hops. Indirect transit regarding the L[th] hop is formed as given in equation (14) and T denotes set of forwarding agents, the criticism creditability of neighbouring hops is signified using C_x^v.

$$(L^d)_x^v(h, h+1) = \begin{cases} \frac{\sum_{b \in T-\{h\}} C_x^v(h,b) * L^{d^z}{}_x(h+1)}{\sum_{b \in T-\{h\}} C_x^v(h,b)} & if\ |T-\{h\}| = 0 \\ 0 & else\ |T-\{h\}| > 0 \end{cases} \quad (14)$$

3.4.3. Estimation of Data Propagation of Nodes

The nodes in a WSN only expend a little amount of energy sensing and transmitting data. By assessing the data from forwarding nodes, it is now feasible to analyse and determine if the node is being attacked or not. The forwarding rate factor is a result.

$$L^{DFR} = \frac{FM^v(h,h+1)}{PS^v(h,h+1)} \quad (15)$$

Where $FM^v(h, h+1)$ denotes number of feedback messages, $PS^v(h, h+1)$ shows the total of data packets needs to be sent, h is the estimation hop and h+1 signifies the hop to be assessed.

3.4.4. An Element of Trustworthiness of Nodes

Every time a packet of information is sent to an adjacent node, the source node checks to see whether it was tampered with, checks to see if it was sent at a specified time, and ensures its reliability and accuracy by equation (16).

$$L^{IF} = \frac{DPF^v(h,h+1)}{PF^v(h,h+1)} \quad (16)$$

Where total number of data packets forwarded by the adjacent nodes is represented by $DPF^v(h, h+1)$ and the data packet to be forwarded to the source node is denoted by $PF^v(h, h+1)$.

The IFTM incorporates reliance of neighbourhood nodes, derived confidence of nodes, estimation of data propagation of nodes and an element of trustworthiness of nodes are four key criteria used to assess a node's trustworthiness. The intuitionistic fuzzy inference model uses these as input and transforms the crisp values into intuitionistic values. The knowledge base gathers data and sends it to the inference engine using the data obtained from the chaos chicken swarm optimization's output. The trust value for the concerned node is provided by the intuitionistic fuzzy inference engine, which constructs a set of intuitionistic fuzzy rules depending on the input received. The computed output is used to determine the trust value of the CH nodes and transient nodes involved in data transmission, and based on that value, the most secure pathways are chosen to achieve optimized data transfer

RESEARCH ARTICLE

between the source and based station in WSN to recognize and defend against attacks like black holes and selective forwarding while data is being transmitted. The workflow of the intuitionistic fuzzy trust model is shown in Figure 7.

3.4.5. Exemplification of Intuitionistic Fuzzy Directions

- When the value of an element of trustworthiness of nodes, derived confidence of nodes, reliance of neighborhood nodes, and estimation of data propagation of nodes is high then automatically the trust value is considered to be high.
- When the value of an element of trustworthiness of nodes, derived confidence of nodes, reliance of neighborhood nodes, and estimation of data propagation of nodes is low then the trust value is considered to be low.
- When the value of an element of trustworthiness of nodes, derived confidence of nodes, reliance of neighborhood nodes, and estimation of data propagation of nodes is average then the trust value is considered to be average.

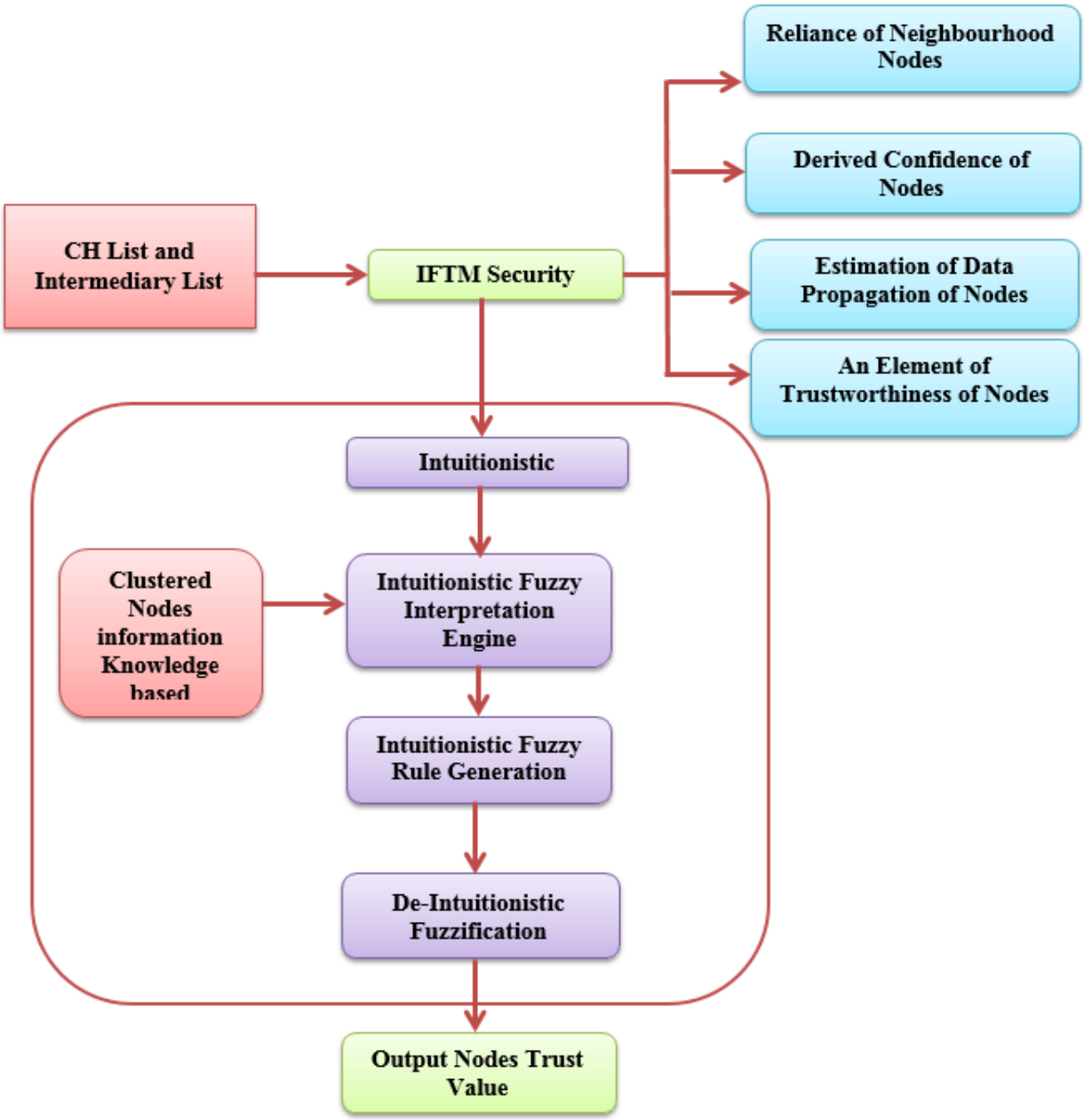

Figure 7 Workflow of Intuitionistic Fuzzification based Trust Model

RESEARCH ARTICLE

4. RESULTS AND DISCUSSION

This section deliberates in detail on a comparative examination of the proposed methodology ECSO+IFTM for energy-aware and secure data transmission by discovering and avoiding SFA and BHA in CWSN. The proposed methodology is simulated using MATLAB software and simulation settings are described in Table 1. A 100 × 100 area is covered with wireless sensor nodes deployed for analysis. The proposed ECSO+IFTM algorithm is compared with the existing approaches such as MW-LEACH [9], TARF [16] protocol, and a Reliable and Dynamic with Energy Aware Routing (RDEAR) [10] protocol. The metrics considered for conducting performance analysis are based on energy consumption analysis, packet delivery ratio analysis, packet loss analysis, and throughput analysis.

Table 1 Simulation Considerations

Parameter	Value	Explanation
SN	150	Number of nodes
E_0	0.5 Joules	Beginning Energy
BS_P	60,60	Base station position
Efs	10 pJ/bit/m2	Short-distance transmission of energy exhausted by the amplifier.
ε_{mp}	0.0013 pJ/bit/m4	To transfer energy over a greater distance, the amplifier must expend more energy.
E_{elec}	50 nJ/bit	The amount of energy used by the circuit either to send or receive the signal.
Packet Size	500 Bytes	Size of a data packet
Message	25 Bytes	Hello or broadcast or cluster head join message

4.1. Energy Consumption Analysis

Whole energy of the network is intended as total of all hop energies, indicating sensor nodes residual energy. Energy requirement stays valuable and constructed as shown in equation (17) as follows:

$$NE = \frac{1}{H}\sum_{L=1}^{H} Eng(J_L) \quad (17)$$

The network energy as formulated in the about equation is used for computing the overall energy for each hop involved in data transmission. The number of hops is signified by H which involves indirect communication or multi-hop routing and $Eng(J_L)$ and represents the energy of L^{th} hop.

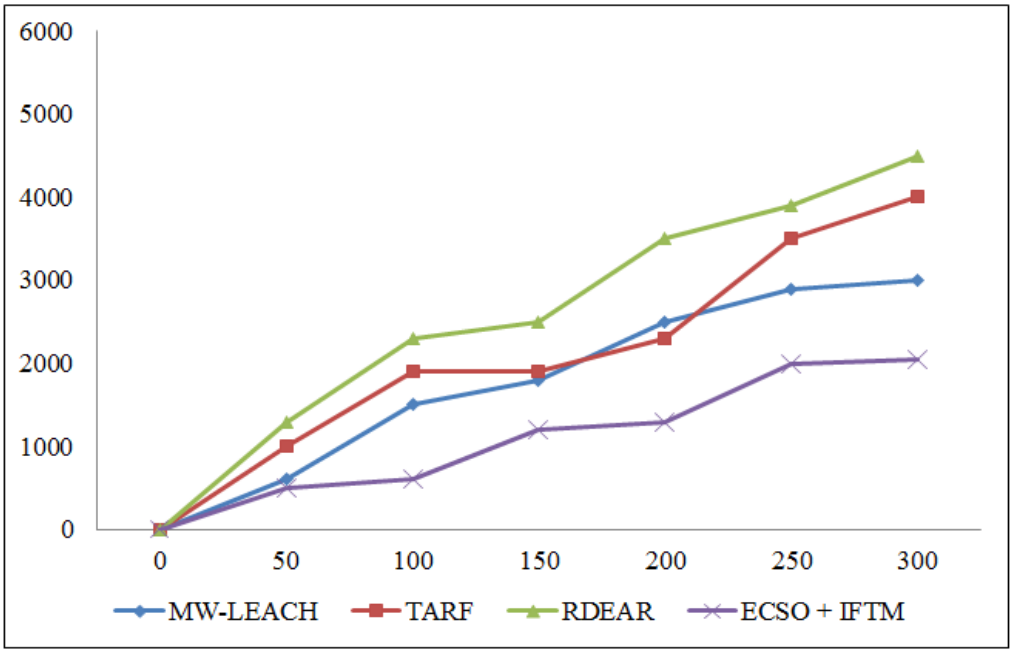

Figure 8 Energy Consumption Analysis

RESEARCH ARTICLE

Figure 8 demonstrates the energy consumption that takes place during the secured data transmission, whereas X-axis signifies node density and Y-axis symbolizes energy consumption during data communication. The result discovers the comparative results of different algorithms in clustering and secure routing. When compared with MW-LEACH, TARF, RDEAR, and proposed ECSO+IFTM, the efficient working of proposed methodology is evident that it outperforms the existing methods with respect to minimal energy consumption. The result also explores the selection of cluster head, transient nodes, and gateways which plays an essential role in data transmission from source node to sink node. For intra-cluster communication, the neighbouring nodes are selected and the route selection of transient nodes and gateway nodes is carried out using the Intuitionistic trust model. The intuitionistic fuzzy handles the indeterminacy in determining the trustworthiness of each hop which involves data transmission accomplished prominently by effectively handling of SFA and BHA.

4.2. Throughput Analysis

It is defined as quantity of data packets received within the given amount of time after which the delivery of each packet is acknowledged as well and it is calculated using equation (18), where NPR refers to total number of packets received and T refers to simulation time.

$$Th = \frac{NPR}{T} \quad (18)$$

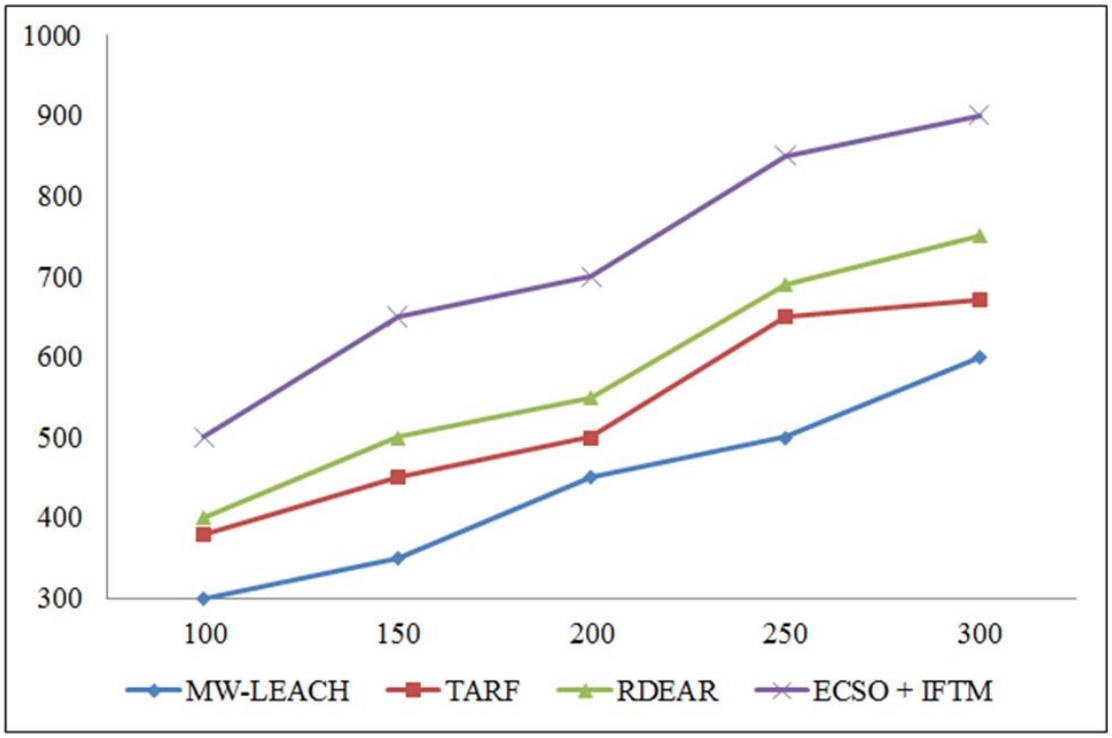

Figure 9 Throughput Analysis

Performance comparison of throughput of proposed ECSO+IFTM with the existing MW-LEACH, TARF, and RDEAR is shown in Figure 9, whereas X-axis signifies network size and Y-axis denotes the throughput of MW-LEACH, TARF, RDEAR, and the proposed work ECSO +IFTM. The proposed methodology provides the highest throughput compared with the existing approaches. ECSO + IFTM are used for the detection, prevention, and recovery of SFA and BHA to provide secure data transmission using multi-hop communication.

The intuitionistic fuzzification is used which determines each intermediate hop in terms of association, indeterminacy, and non-membership affiliation degree. The IFTM trust model extremely well uncovers the issue of uncertainty caused by the unpredictable behaviour of hostile nodes because of Selective forward and black hole attacks, hence its throughput is superior relative to existing approaches.

4.3. Packet Drop Ratio Analysis

In the course of data transmission the amount of packets lost must be kept low. The packet delivery ratio is mathematically represented in equation (19), where TDP^{tx} and TDP^{rx} are the total numbers of packets sent and received, accordingly.

$$P_{DR} = \frac{TDP^{tx} - TDP^{rx}}{TDP^{tx}} \quad (19)$$

RESEARCH ARTICLE

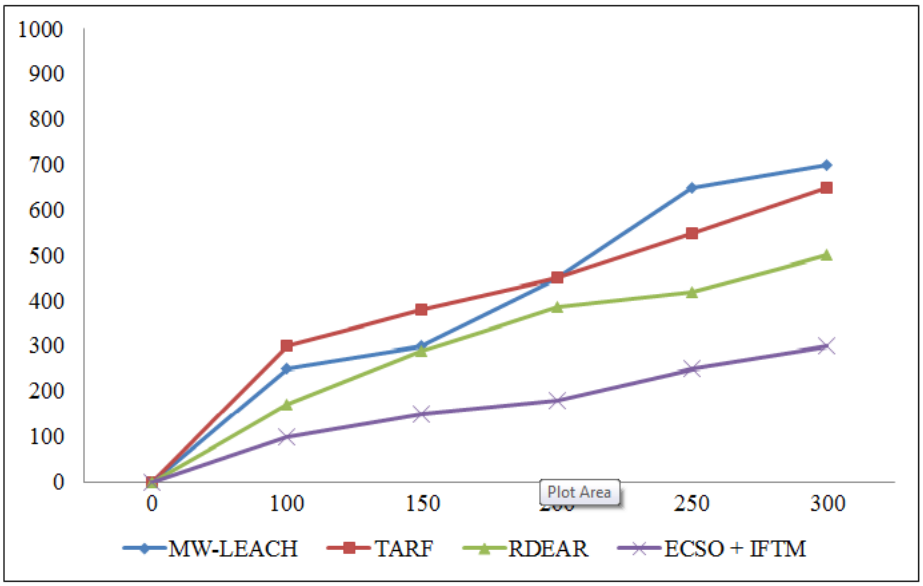

Figure 10 Packet Drop Analysis

Figure 10 displays the comparison of packet drop analysis of the proposed ECSO+IFTM, MW-LEACH, TARF, and RDEAR. In Figure 10, X-axis indicates simulation time and Y-axis symbolizes the packet drop ratio. The results prove that the proposed methodology works efficiently in achieving higher security and energy-aware-based data transfer using multi-hop communication in WSN. The proposed ECSO +IFTM produced the least packet drop ratio as it follows two different factors to improve safe data communication in inter-cluster communication. By using chicken swarm optimization-based clustering, the cluster head is chosen. The hop selection for data transmission is done via an intuitionistic fuzzy trust model. The trust principles of cluster heads, transient nodes, and gateways are computed with the help of an intuitionistic fuzzy trust model. These factors Defence against both selective forwarding and black hole attacks and reduces the packet drop ratio majorly compared with MW-LEACH, TARF, and RDEAR.

4.4. Packet Delivery Ratio Analysis

The relationship of distinctive data packets acquired by the target nodes towards the total quantity of messages provided by source nodes is known as the packet delivery ratio. Let TP represent the entire amount of data packets produced by the source, DP_i represent amount of data packets received successfully by a sink can be represented analytically in the equation (20).

$$DLR = \frac{\sum_{i=1}^{n} DP_i}{TP} \quad (20)$$

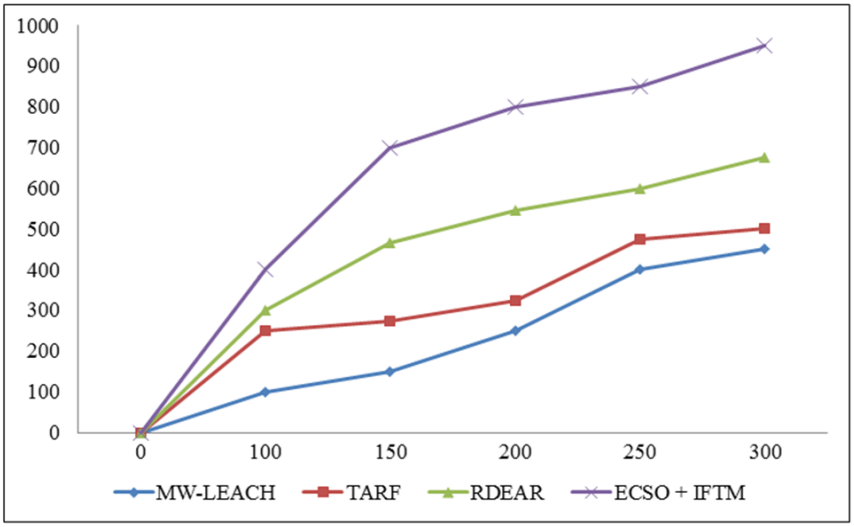

Figure 11 Packet Delivery Analysis

RESEARCH ARTICLE

Figure 11 illustrates the successful routing and data transmission by ECSO+IFTM. In Figure 11, X-Axis indicates the simulation time and Y-Axis indicates the packet delivery ratio. The result obtained as of the proposed methodology is compared with three alternative clustering models used for data transmission in clustered WSN based on the number of packets arrival rate. The prevailing methods MW-LEACH, TARF, and RDEAR are unable to cope with the ambiguity in possible cluster head election and unpredictable conduct of malicious nodes. The proposed methodology provides a high probability of a successful packet delivery ratio than the existing model. By using the nature of intuitionistic fuzzy, ECSO+IFTM emphasizes the trust model. In clustered wireless sensor networks, the forwarding hops are chosen based on the fitness value of CSO algorithm.

5. CONCLUSION

The proposed methodology combines an energy-efficient selection of cluster head, assistant cluster head, gateway nodes, and cluster members to establish secure and energy-aware inter-cluster communication. This also helps in detecting, preventing, and recovering from the occurrence of selective forwarding and black hole attacks which results in the improvement of security mechanisms. According to the simulation results, ECSO+IFTM performs in an improved way in terms of attaining maximum throughput, high packet delivery ratio, low packet drop, and minimal energy consumption in inter-cluster communication when compared with the existing approaches such as the MW-LEACH, TARF, and RDEAR. Meantime, the proposed methodology proficiently decreases cluster head failure and improves with the advanced choosing assistant cluster head helps in reducing maintenance cost of the clusters. The chaos chicken flock optimization's nodes are grouped in a hierarchical arrangement with the strongest node serving as the cluster head and the remaining nodes acting as transitory nodes for transmitting data created by the source to its destination. The nodes are sorted according to their fitness value which depends on their residual energy and nodes density which is designed as roosters have the highest fitness values determined using chicken fitness value computation. The local optima were handled using the chaotic nature induced in this algorithm. The nominated cluster leader is in charge of data transformation and consolidation. By the trust values produced by the intuitionistic fuzziness values, the secure path is chosen. Based on the evaluation metrics used for performance analysis in this work, the experimental results proved that proposed methodology ECSO+IFTM achieves the highest network performance in accomplishing energy aware and secure transfer by defencing SFA and BHA in Cluster-Based WSN. In future, the proposed methodology can be improved with an additional algorithm for providing energy-aware and secure routing in Internet of Things (IoT) enabled environment.

REFERENCES

[1] M. Jain and H. Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks," in International Conference Advances in Computing, Control, and Telecomm. Technologies (ACT '09), pp. 555-558 (2009).

[2] He Z, Chen L, Li F, Jin G (2023) A fuzzy model for content-centric routing in Zigbee-based wireless sensor networks (WSNs). PLoS ONE 18(6): e0286913. https://doi.org/10.1371/journal.pone.0286913

[3] Sathish kumar, R., Ramesh C, "A modified method for preventing black-hole attack in mobile ad hoc networks," in J. Eng. Appl. Sci. 11(2), 182–191 (2016)

[4] M. Shinde and D. C. Mehetre, "Black Hole and Selective Forwarding Attack Detection and Prevention in WSN," in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, pp. 1-6,(2017).

[5] Saleh, A.; Joshi, P.; Rathore, R.S.; Sengar, S.S. Trust-Aware Routing Mechanism through an Edge Node for IoT-Enabled Sensor Networks. Sensors 2022, 22, 7820. https://doi.org/10.3390/s22207820

[6] Yao, Y., Chen, W., Guo, J. et al. Simplified clustering and improved intercluster cooperation approach for wireless sensor network energy balanced routing. J Wireless Com Network 2020, 131 (2020). https://doi.org/10.1186/s13638-020-01748-8

[7] Srinivas, T. A., S-S, M, "Black Hole and Selective Forwarding Attack Detection and Prevention in IoT in Health Care Sector: Hybrid meta-heuristic-based shortest path routing," in Journal of Ambient Intelligence and Smart Environments, 13(2):133–156, (2021).

[8] C. Lai, H. Li, R. Lu and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," in Comput. Netw., vol. 57, no. 17, pp. 3492-3510, December (2013).

[9] El Khediri, Salim Khan, Rehanullah Nejah, Nasri Kachouri, Abdennaceur, "MW-LEACH: Low energy adaptive clustering hierarchy approach for WSN," in IET Wireless Sensor Systems. Vol 10(4), (2020).

[10] Hicham Qabouche, Aicha Sahel, Abdelmajid Badri, and Ilham El Mourabit, "Novel Reliable and Dynamic Energy-Aware Routing Protocol for Large Scale Wireless Sensor Networks," in International Journal of Electrical and Computer Engineering, ISSN: 2088-8708, Vol. 12, No. 6, Decemeber 2022, pp. 6440-6448.

[11] S. Srinivasa Rao, K. Chenna Keshava Reddy and S. Ravi Chand (2022), A Novel Optimization based Energy Efficient and Secured Routing Scheme using SRFIS-CWOSRR for Wireless Sensor Networks. IJEER 10(3), 644-650. DOI: 10.37397/IJEER.100338.

[12] Mehetre, D.C., Roslin, S.E. & Wagh, S.J, " Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," in Cluster Comput 22 (Suppl 1), 1313–1328 (2019).

[13] Yadav R. K., & Mahapatra R. P. (2021). Energy aware optimized clustering for hierarchical routing in wireless sensor network. Computer Science Review, 41, 100417

[14] A. Mehbodniya, S. Bhatia, A. Mashat, M. Elangovan and S. Sengan, "Proportional fairness based energy efficient routing in wireless sensor network," Computer Systems Science and Engineering, vol. 41, no.3, pp. 1071–1082, 2022.

[15] Vinodhini R., & Gomathy C. (2021). Fuzzy Based Unequal Clustering and Context-Aware Routing Based on Glow-Worm Swarm Optimization in Wireless Sensor Networks: Forest Fire Detection. Wireless Personal Communications, 118(4), 3501–3522.

[16] Udhayavani, M., & Chandrasekaran, M. (2019). Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: A trust-aware routing framework for wireless sensor networks. Cluster Computing, 22(5), 11919-11927.

[17] Meng, X., Liu, Y., Gao, X., Zhang, H. (2014). A New Bio-inspired Algorithm: Chicken Swarm Optimization. In: Tan, Y., Shi, Y., Coello, C.A.C. (eds) Advances in Swarm Intelligence. ICSI 2014. Lecture Notes in Computer Science, Vol. 8794. Springer

[18] Smith, C.L., Zielinski, S.L.: The Startling Intelligence of the Common Chicken. Scientific American 310(2) (2014).

RESEARCH ARTICLE

[19] Gehad Ismail Sayed, Alaa Tharwat and Aboul Ella Hassanien, "Chaotic dragonfly algorithm: an improved metaheuristic algorithm for feature selection" in Journal: Applied Intelligence, Volume 49, Number 1, Page 188 (2019).
[20] Wang, Zhenwu, Chao Qin, Benting Wan, William Wei Song, and Guoqiang Yang. "An adaptive fuzzy chicken swarm optimization algorithm." Mathematical Problems in Engineering 2021 (2021): 1-17.
[21] Atanassov K.T, "Intuitionistic Fuzzy Sets" in Fuzzy Sets Syst. 1986; 20:87–96.
[22] Xu Z., Yager R.R, "Some Geometric Aggregation Operators Based on Intuitionistic Fuzzy Sets," in Int. J. Gen. Syst. 2006; 35:417–433.
[23] Shen F., Ma X., Li Z., Xu Z., Cai D, " An Extended Intuitionistic Fuzzy TOPSIS Method Based on a New Distance Measure with an Application to Credit Risk Evaluation," in Inf. Sci. 2018; 428:105–119.

Authors

A. Anitha received her Bachelor's degree in Information Technology, Master's degree in Computer Technology and M.Phil in Computer Science from Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India in 2011, 2013 and 2017 respectively. She is currently pursuing her Ph.D in field of Computer Networks with Dr.S.Mythili at Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India. She has published 5 research papers in International Journals and 1 book chapter in Lecture Notes in Networks and Systems. She has presented papers in National and International Conferences and also participated in Webinars. She completed Introduction to Cybersecurity course from CISCO Networking Academy. Her research interests include Wireless Sensor Networks, Wireless Adhoc Networks, Network Routing and Security.

Dr. S. Mythili working as Dean, School of Computer Science, Associate Professor and Head, Department of Information Technology, Kongunadu Arts and Science College, has about 20 Years of experience in academic and research. She has completed her under graduate degree from Avinashiligam Institute for Home Science and Higher Education for Women and thereafter completed her Master of Computer Applications (MCA) and M.Phil from Kongunadu Arts and Science College. She has completed her Ph.D from Bharathiar University and has qualified UGC - National Level Eligibility Test (NET) and State Level Eligibility Test (SET). She is a Life Member of Indian Science Congress Association. Her research area is Detection of Clones in Programming Language Paradigms and Model Driven Architectures. She has published 21 research papers in reputed International Journals and in 7 Conferences out of which 9 Publications are in Scopus and 1 publication in Science Citation Index. To her credit she has published 3 National Patent and one International Patent. She has organized various National/ International Conferences Seminars and workshops. She has been a member in Board of studies in other colleges and universities and has also served as resource person in various colleges. Her current area of interest is Software Engineering and Data Mining. She has guided 6 Research Scholars for M.Phil and currently guiding 4 Ph.D Research scholars.

How to cite this article:

A. Anitha, S. Mythili, "Empowered Chicken Swarm Optimization with Intuitionistic Fuzzy Trust Model for Optimized Secure and Energy Aware Data Transmission in Clustered Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 10(4), PP: 511-526, 2023, DOI: 10.22247/ijcna/2023/223311.