The Scientific Temper (2024) Vol. 15 (spl): 275-282

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.32

https://scientifictemper.com/

RESEARCH ARTICLE

Fuzzy optimization trust aware clustering approach for the detection of malicious node in the wireless sensor networks

A. Rukmani*, C. Jayanthi

Abstract

Wireless sensor networks (WSNs) are pivotal in various applications, ranging from environmental monitoring to military operations. However, their susceptibility to security threats, particularly from malicious nodes, poses significant challenges to network integrity and data reliability. This paper proposes an innovative methodology that integrates clustering with an optimization approach to effectively identify and mitigate malicious nodes in WSNs. In the proposed methodology, the network is divided into clusters, each managed by a cluster head responsible for monitoring the behavior of nodes within its cluster. Trust values are assigned to nodes based on parameters such as data forwarding accuracy, communication consistency, and energy consumption. These trust metrics are optimized using a sophisticated optimization algorithm, which fine-tunes the decision-making process for identifying malicious nodes. By leveraging clustering, the method efficiently distributes computational tasks, while the optimization algorithm enhances the accuracy of malicious node detection by dynamically adjusting trust thresholds. The approach not only reduces the incidence of false positives but also extends the network lifetime by preventing compromised nodes from disrupting network operations. This trust-aware, optimized clustering strategy offers a robust solution for securing WSNs in critical applications, ensuring reliable and secure data transmission across the network.

Keywords: Wireless sensor network, Malicious node, Clustering approach, Optimization algorithm, Cluster formation, Packet delivery ratio.

Introduction

Wireless sensor networks (WSNs) have become an integral part of modern technology, enabling a wide range of applications, including environmental monitoring, military surveillance, smart cities, and healthcare. These networks consist of spatially distributed sensor nodes that collaborate to collect and transmit data to a central base station or gateway. Despite their numerous advantages, WSNs are inherently vulnerable to various security threats, particularly from malicious nodes that can compromise the integrity, confidentiality, and availability of the network. Detecting and mitigating these malicious nodes is a critical challenge that requires innovative approaches, Wang, C., Liu, G., & Jiang, T. (2024); Arab, A. (2023).

Traditional security mechanisms, such as cryptography and authentication, are often insufficient for WSNs due to their resource-constrained nature. The limited computational power, memory, and energy capacity of sensor nodes necessitate lightweight and efficient security solutions. Moreover, the dynamic and decentralized architecture of WSNs makes them susceptible to a range of attacks, including node capture, data tampering, and Sybil attacks, which can lead to network disruption and inaccurate data collection, Sabitha, R., Prasad, C. G., & Karthik, S. (2023), Faris, M., Mahmud, M. N., Salleh, M. F. M., & Alnoor, A. (2023).

To address these challenges, this paper proposes a novel methodology that integrates a clustering approach with an optimization algorithm for the effective identification of malicious nodes in WSNs. Clustering techniques are employed to organize the sensor nodes into manageable groups or clusters, where a cluster head oversees each cluster. This hierarchical structure not only enhances the

PG and Research Department of Computer Science, Government Arts College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli – 24), Karur, Tamil Nadu, India.

***Corresponding Author:** A. Rukmani, PG and Research Department of Computer Science, Government Arts College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli – 24), Karur, Tamil Nadu, India, E-Mail: eswarruby@gmail.com

How to cite this article: Rukmani, A., Jayanthi, C. (2024). Fuzzy optimization trust aware clustering approach for the detection of malicious node in the wireless sensor networks. The Scientific Temper, **15**(spl):275-282.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.32

Source of support: Nil

Conflict of interest: None.

© The Scientific Temper. 2024

Received: 07/09/2024 **Accepted:** 23/09/2024 **Published:** 16/10/2024

network's scalability and energy efficiency but also facilitates localized monitoring and detection of suspicious activities within each cluster, Wajgi, D. W., & Tembhurne, J. V. (2024), Debasis, K., Sharma, L. D., Bohat, V., & Bhadoria, R. S. (2023).

The optimization algorithm, on the other hand, plays a pivotal role in fine-tuning the trust evaluation and clustering parameters. By optimizing factors such as trust thresholds, cluster head selection, and node behavior analysis, the proposed methodology improves the accuracy of malicious node detection while minimizing false positives and energy consumption. The integration of clustering and optimization allows for a balanced approach that leverages the strengths of both techniques, ensuring a robust and efficient security solution for WSNs, Subedi, S., Acharya, S. K., Lee, J., & Lee, S. (2024, June).

This paper outlines the design and implementation of the proposed methodology, followed by an evaluation of its performance through simulations. The results demonstrate the effectiveness of the approach in detecting malicious nodes, extending network lifetime, and maintaining reliable data transmission in the presence of security threats. The proposed methodology represents a significant advancement in the field of WSN security, offering a scalable, energy-efficient, and accurate solution for safeguarding critical sensor networks against malicious activities, Mutar, M., & Hammood, D. A. (2023).

Background Study

WSNs are composed of numerous sensor nodes that collaborate to monitor and report environmental conditions in a distributed manner. These networks are widely deployed in diverse fields such as environmental monitoring, healthcare, military applications, and smart infrastructure due to their ability to provide real-time data collection and analysis. However, the open and often unattended nature of WSNs makes them highly susceptible to various security threats, especially from malicious nodes. Understanding the nature of these threats and the existing methods to counteract them is essential to developing more robust solutions, Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023).

Security Challenges in WSNs

WSNs operate under stringent resource constraints, including limited energy supply, computational power, and memory capacity. These limitations, combined with the wireless communication medium, make WSNs particularly vulnerable to a wide range of attacks. Malicious nodes can infiltrate the network through various means, such as node capture, where an attacker physically compromises a sensor node and reprograms it to behave maliciously, Hassan, K., Madkour, M. A., & Nouh, S. A. (2023).

Other common attacks include:

- *Sybil attacks*

Where a single node presents multiple identities to the network, disrupting routing protocols and trust mechanisms.

- *Wormhole attacks*

In which an attacker records packets at one location and replays them at another, leading to routing misdirection.

- *Selective forwarding attacks*

Where a compromised node selectively drops or alters packets, leading to inaccurate data reporting.

Existing Security Mechanisms

Traditional security mechanisms, such as encryption and authentication, offer a degree of protection but are often insufficient in WSNs due to their resource-intensive nature. Moreover, WSNs' dynamic and distributed architecture necessitates lightweight security solutions that can operate effectively under resource constraints. To address these limitations, various strategies have been proposed, including:

- *Trust-based mechanisms*

These approaches evaluate the trustworthiness of nodes based on their behavior, such as packet forwarding reliability, communication consistency, and energy usage. Nodes with low trust scores are flagged as potentially malicious, Liu, J., & Xu, F. (2023, April).

- *Clustering techniques*

Clustering is a common method used to enhance the scalability and energy efficiency of WSNs. In a clustered network, sensor nodes are grouped into clusters, each managed by a cluster head. Clustering reduces communication overhead and allows for localized monitoring, making it easier to detect anomalies at the cluster level, Mutar, M., & Hammood, D. A. (2023).

- *Intrusion detection systems (IDS)*

IDSs are designed to monitor network traffic and node behavior to identify signs of malicious activity. These systems often incorporate anomaly detection methods, which flag deviations from normal behavior patterns as potential threats.

Fuzzy c-means clustering

Fuzzy C-means (FCM) is a soft clustering algorithm that allows data points to belong to multiple clusters with varying degrees of membership. Unlike hard clustering algorithms like K-Means, which assign each data point to a single cluster, FCM assigns a membership value to each data point for each cluster. This membership value indicates the degree to which a data point belongs to a particular cluster. FCM is particularly useful in scenarios where the boundaries between clusters are not well-defined or when overlapping clusters are expected, Sikarwar, N., & Tomar, R. S. (2023),

Panwar, A., & Nanda, S. J. (2023, December).

Key Concepts of Fuzzy C-Means Clustering Approach

Clusters and Centroids:

- Clusters are groups of data points that share similar characteristics.
- Centroids represent the center of a cluster. In FCM, each cluster is associated with a centroid, which is a point in the feature space.

Membership Values

Each data point is associated with a membership value for each cluster, ranging between 0 and 1. The sum of the membership values of a data point across all clusters equals 1.

Fuzziness Parameter (m)

The fuzziness parameter, denoted by m, controls the degree of fuzziness of the resulting clusters. A higher value of m increases the fuzziness, allowing for more overlap between clusters. Typically, m is set to a value greater than 1, often between 1.5 to 2.

Algorithm for Fuzzy C – Means clustering

The FCM algorithm operates iteratively and typically follows these steps:

Step 1: Initialization

- Choose the number of clusters C $(where\ C \geq 2)$.
- Initialize the membership matrix U, where each element. u_{ij} represents the membership value of data point x_i in the cluster j. The matrix is typically initialized with random values, ensuring that the sum of memberships for each data point across all cluster is 1.

Step 2: Centroid calculation

Calculate the centroid v_j of each cluster j using the following formula:

$$v_j = \frac{\sum_{i=1}^{N} u_{ij}^{m} . x_i}{\sum_{i=1}^{N} u_{ij}^{m}} \qquad (1)$$

Where v_j is the centroid of cluster j, N is the total number of data points, x_i is the ith data point, u_{ij} is the membership value of data point x_i in the cluster j, and m is the fuzziness parameter.

Step 3: Membership matrix update

Update the membership values of each data point using the following formula:

$$u_{ij} = \frac{1}{\sum_{k=1}^{C} \left(\frac{\|x_i - v_j\|}{\|x_i - v_k\|} \right)^{\frac{2}{m-1}}} \qquad (2)$$

Where $\| x_i - v_j \|$ is the Euclidean distance between data point x_i and centroid v_j. is an index over all clusters.

Step 4: Convergence check

Compute the difference between the updated membership matrix and the previous one. If the difference is less than a predefined threshold, the algorithm has converged, and the process stops. Otherwise, go back to Step 2. Calculate the change in the membership matrix ΔU from the previous iteration:

$$\Delta U = \left\| U^{(t+1)} - U^{(t)} \right\| \qquad (3)$$

Where $U^{(t+1)}$ and $U^{(t)}$ are the membership matrices at iterations t+1, and t respectively. If $\Delta U < \in$ (convergence threshold) or the number of iterations exceeds max_iter then stop the iteration.

Step 5: Output the final centroids and membership matrix

After convergence, the final cluster centroids V= {v_1,v_2,… ,v_C } and the membership matrix U are output.

Step 6: Cluster assignment

Optionally, assign each data point x_i to the cluster with the highest membership values:

$$Cluster\ (x_i) = \arg\max_j u_{ij} \qquad (4)$$

Harris Hawks Optimization

Harris Hawks Optimization (HHO) is a nature-inspired optimization algorithm introduced by Seyedali Mirjalili in 2019. The algorithm is inspired by the cooperative hunting strategy of Harris's hawks, a bird species known for its group hunting techniques. HHO mimics the dynamic and intelligent behaviors of these hawks during the process of chasing prey, utilizing both exploration and exploitation phases to find the optimal solution in a given search space, Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O. I., Selvaraj, D., & Abdulsahib, G. M. (2023), Hu, H., Fan, X., & Wang, C. (2024).

Key Concepts

Exploration and exploitation

- Exploration refers to the process of broadly searching the solution space to find promising areas, while exploitation involves intensively searching those areas to refine the best solution.
- HHO balances these two phases to avoid getting trapped in local minima and to ensure a thorough search of the solution space.

Harris hawks hunting strategy

Harris's hawks hunt in groups using various strategies depending on the prey's behavior. These strategies include surprise pounce, soft besiege, hard besiege, and others. The HHO algorithm models these strategies through mathematical operators that guide the search process.

Algorithm for HHO

The HHO algorithm consists of three main phases:

Exploration phase (Searching for Prey)

- At the start, hawks (candidate solutions) randomly explore the search space. The positions of the hawks are updated based on a Lévy flight distribution or based on the position of the prey (the best solution found so far).
- This phase allows the Hawks to cover a wide area of the search space to identify regions where the optimal solution might exist.

Transition from exploration to exploitation (Based on the energy of prey)

- As the search progresses, the algorithm monitors the energy of the prey, which decreases as the hawks get closer to it. This energy is modeled using a decreasing function over iterations.
- The transition from exploration to exploitation occurs gradually as the prey's energy decreases, leading to more focused searching near promising solutions.

Exploitation phase (Attacking the Prey)

In this phase, hawks execute one of several strategies to capture the prey. The choice of strategy depends on the prey's energy level and behavior.

- *Soft besiege*

When the prey is still strong, the hawks surround it gradually, allowing for a fine-tuned search for the best solution.

- *Hard besiege*

When the prey is weak, the hawks converge quickly on it, which corresponds to an aggressive search in the vicinity of the best solution.

- *Surprise pounce*

Hawks may suddenly leap toward the prey using a rapid dive, reflecting a large step in the search space toward the best-known solution.

- *Teamwork*

Hawks may work together to besiege the prey, combining information from multiple hawks to refine the solution.

Mathematical Formulation of HHO

Step 1: Initialization

Initialize the population of hawks (candidate solutions) randomly in the search space. Determine the fitness of each hawk based on the objective function.

Step 2: Iteration Process

- *Step 2.1: Exploration phase*

Update the position of each hawk using the formula:

$$X^{t+1} = X^t + J(X^t - X^t_{best}) + S(Levy) \qquad (5)$$

Where $X^{(t+1)}$ is the new positions of the hawks. J and S are random vectors that control the influence of the prey and Lévy flight, respectively. X^t_{best} is the position of the best hawk (prey) at iteration t.

- *Step 2.2: Transition and exploitation phase*

As the iterations progress, calculate the energy of the prey E using:

$$E = 2E_0\left(1 - \frac{t}{T}\right) \qquad (6)$$

Where E_0 is the initial energy, t is the current iteration, T is the maximum number of iterations, and depending on E, decide whether to continue exploration or to switch to one of the exploitation strategies (soft besiege, hard besiege, etc). For exploitation, update the position using specific strategies:

- Soft Besiege: $X^{t+1} = X^t_{best} + r|X^t_{best} - X^t|$ (7)
- Hard Besiege: $X^{t+1} = X^t_{best} - r|X^t_{best} - X^t|$ (8)
- Surprise Besiege: $X^{t+1} = X^t_{best} + Levy$ (9)

Step 2.3: Fitness Evaluation

Evaluate the fitness of each new position and update the best hawk (prey) position if a better solution is found.

Step 3: Convergence

Repeat the iteration process until the maximum number of iterations is reached or the solution has converged to an acceptable level of fitness.

Step 4: Output

The final position of the best hawk represents the optimal solution found by the algorithm.

Proposed Fuzzy Optimization Trust Aware Clustering (FOTAC) Approach for the Detection of Malicious Nodes in WSN

The proposed approach combines Fuzzy C-Means (FCM) clustering and Harris Hawks Optimization (HHO) to create a robust, trust-aware mechanism for detecting malicious nodes in Wireless Sensor Networks (WSNs). The approach leverages FCM for soft clustering based on trust metrics and employs HHO to optimize the clustering process, ensuring effective identification and isolation of malicious nodes.

The following are the step-by-step procedures for the optimization-based Trust Aware Clustering (FOTAC) approach.

Step 1: Initialize the network and parameters

- Deploy sensor nodes in the wireless sensor network (WSN).
- Initialize the parameters for Fuzzy C-means (FCM) clustering and the trust model.
- Set up the initial trust values for each node based on prior knowledge or baseline behavior (packet forwarding rate, energy consumption, communication history).

- Initialize the population of hawks (candidate solutions) and parameters for Harris Hawks optimization (HHO), including the number of hawks, maximum iterations, and initial prey energy.

Step 2: Fuzzy C-Means clustering based on trust metrics

Apply the Fuzzy C-Means (FCM) algorithm to group the nodes into clusters based on trust metrics. The nodes are assigned membership degrees to each cluster using the trust values computed from their behavior, energy, and communication attributes.

$$J(U,V) = \sum_{i=1}^{N}\sum_{j=1}^{C} u_{ij}^{m}\left\|x_i - v_j\right\|^2 \quad (10)$$

Where N is the number of node, C is the number of clusters, u_{ij} is the membership degree of node x_i in cluster j, v_j is the centroid of cluster j, and m is the fuzziness parameters.

Step 3: Trust calculation for each node

Calculate the trust value for each node using a combination of packet forwarding behavior, energy consumption, and communication reliability. Where $\alpha_1,\alpha_2,\alpha_3$ are weight coefficients, and each trust factor is computed as follows:

$$T_i = \alpha_1 \times T_{behaviour} + \alpha_1 \times T_{energy} + \alpha_3 \times T_{communication} \quad (11)$$

- Behavior Trust: $T_{behaviour} = \frac{Successful\ Forwarding\ Events}{Total\ Forwarding\ Events}$ (12)
- Energy Trust : $T_{energy} = 1 - \frac{E_{Consumed}}{E_{initial}}$ (13)
- Communication Trust: $T_{communication} = \frac{Successful\ Forwarding\ Events}{Total\ Forwarding\ Events}$ (14)

Step 4: harris hawks optimization (HHO) for cluster optimization

- Apply the Harris Hawks optimization (HHO) algorithm to optimize the clustering process by fine-tuning the positions of the nodes and the centroids of the clusters.
- Hawks (candidate solutions) update their positions to optimize the objective function based on the trustworthiness of nodes within the clusters.
- Update the position using equation (7) (8) (9). Update the energy (6), and Levy Fight Distribution with equation $Levy(X) = X + \alpha.\frac{s}{|u|^{\frac{1}{\beta}}}$. Where s and u are normally distributed random numbers, α is a scaling factor, and is a distribution parameter.

Step 5: Fitness evaluation

The fitness of each hawk (solution) is evaluated based on the trust values of the nodes within each cluster. The objective is to maximize the trust within each cluster while minimizing the detection of false positives.

Step 6: Update of hawk positions

Based on the fitness evaluation, update the positions of the hawks using the HHO strategy, moving towards the optimal solution in terms of clustering the nodes into high-trust clusters.

Step 7: Detection of malicious nodes

- After the optimization process, nodes with low trust values across iterations are flagged as potential malicious nodes.
- Isolate these nodes from the network to prevent further malicious activity.

Step 8: Continuous monitoring and re-optimization

Continuously monitor the network for changes in node behavior. Recalculate trust values periodically and reapply the clustering and optimization process to adapt to dynamic network conditions.

Result And Discussion

The performance of the proposed FOTAC is evaluated with the existing clustering approaches like Fuzzy C-means (FCM), weighted clustering (WC), and K-means (KM) clustering. The performance of the proposed FOTAC is evaluated with performance metrics like packet delivery ratio (in %), packet loss (in %), end-to-end delay (in %), energy consumption (in Joules) and throughput (in mpbs) with varying percentages of sybil nodes in the network.

Performance Analysis with 5% Malicious Nodes in the WSN

Table 1 depicts the Packet Loss (in %) obtained by the Proposed FOTAC, FCM, WC and KM Clustering techniques with 5% sybil nodes in the network. From Table 1, it is clear that the proposed FOTAC approach reduced the packet loss than the other clustering techniques.

Table 2 depicts the packet delivery ratio (in %) obtained by the proposed FOTAC, FCM, WC and KM Clustering techniques with 5% sybil nodes in the network. From Table 2, it is clear that the proposed FOTAC approach gives an improved packet delivery ratio than the other clustering techniques.

Table 3 depicts the end-to-end delay (in %) obtained by the proposed FOTAC, FCM, WC and KM Clustering

Table 1: Packet loss (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 5% sybil nodes in the network

Number of nodes	*Packet loss (in %)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	14.36	15.58	15.96	16.77
125	15.47	18.25	18.99	19.42
150	16.85	19.31	20.74	21.17
175	17.64	20.08	20.98	21.78
200	18.83	22.74	23.47	24.76
225	19.32	23.41	24.11	25.36
250	20.07	23.85	25.47	26.63
275	21.45	24.13	25.86	27.74
300	22.52	25.61	26.77	28.82

Table 2: Packet delivery ratio (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 5% sybil nodes in the network

Number of nodes	*Packet delivery ratio (in %)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	93.74	91.42	90.88	89.25
125	92.81	90.55	89.77	88.63
150	91.22	89.36	88.47	87.11
175	90.55	88.25	87.41	86.63
200	89.63	87.58	86.12	85.74
225	88.52	86.21	85.36	84.42
250	88.03	85.72	84.35	83.55
275	86.22	84.29	83.64	82.17
300	85.52	83.25	82.46	81.44

Table 3: End-to-end delay (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 5% sybil nodes in the network

Number of nodes	*End-to-end delay (in %)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	12.58	13.63	14.47	15.54
125	13.99	14.84	15.32	16.42
150	14.45	15.73	16.62	17.53
175	15.61	16.43	17.92	18.75
200	16.97	17.36	18.85	19.93
225	17.82	18.73	19.52	20.17
250	18.91	19.54	20.82	21.91
275	19.88	20.71	21.45	22.69
300	20.96	21.77	22.82	23.46

techniques with 5% sybil nodes in the network. From Table 3, it is clear that the proposed FOTAC approach gives reduces the End-to-End Delay than the other clustering techniques.

Table 4 depicts the average energy consumption (in Joules) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 5% sybil nodes in the network. From Table 4, it is clear that the proposed FOTAC approach gives reduced average energy consumption (in joules) than the other clustering techniques.

Table 5 depicts the throughput (in mbps) obtained by the proposed FOTAC, FCM, WC and KM Clustering techniques with 5% sybil nodes in the network. From Table 4, it is clear that the proposed FOTAC approach gives improved throughput (in mbps) than the other clustering techniques.

Performance Analysis with 15% Malicious Nodes in the WSN

Table 6 depicts the packet loss (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 15% sybil nodes in the network. From Table 6, it is clear that the proposed FOTAC approach reduced the packet loss than the other clustering techniques.

Table 4: Average energy consumption (in Joules) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 5% sybil nodes in the network

Number of nodes	*Average energy consumption (in Joules)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	0.1	0.12	0.15	0.17
125	0.16	0.18	0.19	0.21
150	0.19	0.21	0.22	0.23
175	0.26	0.28	0.29	0.31
200	0.28	0.31	0.33	0.35
225	0.31	0.33	0.35	0.37
250	0.39	0.42	0.45	0.48
275	0.48	0.51	0.53	0.56
300	0.57	0.59	0.61	0.64

Table 5: Throughput (in mbps) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 5% sybil nodes in the network

Number of nodes	*Throughput (in mbps)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	1274	1145	1123	1098
125	1163	1058	998	932
150	971	884	802	784
175	898	742	696	621
200	791	674	598	503
225	662	594	493	452
250	652	532	484	396
275	573	493	375	322
300	501	451	394	313

Table 6: Packet loss (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 15% sybil nodes in the network

Number of nodes	*Packet loss (in %)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	32.36	33.96	34.42	35.59
125	33.53	34.21	35.74	36.98
150	34.72	35.88	36.14	37.73
175	35.45	36.43	37.25	38.36
200	36.61	37.13	38.88	39.74
225	37.41	38.94	39.45	40.14
250	38.51	39.96	40.72	41.75
275	39.49	40.86	41.44	42.26
300	40.74	41.69	42.26	43.39

Table 7 depicts the packet delivery ratio (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 15% sybil nodes in the network. From Table 2, it is clear that the proposed FOTAC approach gives an improved packet delivery ratio than the other clustering techniques.

Table 7: Packet delivery ratio (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 15% sybil nodes in the network

Number of nodes	*Packet delivery ratio (in %)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	70.62	69.63	68.88	67.96
125	69.58	68.25	67.76	66.47
150	68.26	67.96	66.58	65.41
175	67.74	66.58	65.84	63.52
200	66.43	65.84	64.88	62.41
225	65.36	64.93	62.564	61.39
250	64.75	62.52	59.92	58.11
275	62.41	60.83	58.41	56.74
300	55.71	50.52	49.74	47.05

Table 8: End-to-end delay (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 15% sybil nodes in the network

Number of nodes	*End-to-end delay (in %)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	33.29	34.96	35.77	34.25
125	34.69	36.75	37.94	38.96
150	35.83	37.69	38.45	39.22
175	36.39	40.74	41.63	42.89
200	37.82	42.96	43.54	44.13
225	38.32	43.74	44.98	45.63
250	39.74	44.23	45.73	46.85
275	40.36	45.55	46.28	47.96
300	41.47	46.85	48.36	49.52

Table 9: Average energy consumption (in Joules) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 5% sybil nodes in the network

Number of nodes	*Average energy consumption (in Joules)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	0.12	0.22	0.25	0.29
125	0.18	0.31	0.33	0.39
150	0.21	0.42	0.48	0.49
175	0.29	0.51	0.53	0.56
200	0.31	0.59	0.61	0.63
225	0.38	0.64	0.69	0.71
250	0.48	0.73	0.76	0.80
275	0.55	0.81	0.83	0.87
300	0.63	0.89	0.91	0.92

Table 8 depicts the end-to-end delay (in %) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 15% sybil nodes in the network. From Table 3, it is clear that the proposed FOTAC approach reduced the end-to-end delay than the other clustering techniques.

Table 10: Throughput (in mbps) obtained by the proposed FOTAC, FCM, WC and KM clustering techniques with 15% sybil nodes in the network

Number of nodes	*Throughput (in mbps)*			
	Proposed FOTAC	*FCM*	*WC*	*KM*
100	1096	998	941	896
125	958	814	798	736
150	749	701	699	621
175	697	656	596	498
200	632	585	496	452
225	592	473	412	398
250	489	389	374	356
275	524	312	298	274
300	485	284	263	216

Table 9 depicts the average energy consumption (in Joules) obtained by the proposed FOTAC, FCM, WC and KM Clustering techniques with 15% sybil nodes in the network. From Table 4, it is clear that the proposed FOTAC approach gives reduced average energy consumption (in joules) than the other clustering techniques.

Table 10 depicts the throughput (in mbps) obtained by the proposed FOTAC, FCM, WC and KM Clustering techniques with 15% sybil nodes in the network. From Table 4, it is clear that the proposed FOTAC approach gives improved throughput (in mbps) than the other clustering techniques.

Conclusion

The proposed optimization-based fuzzy trust-aware clustering (FOTAC) approach using Harris Hawks optimization (HHO) and Fuzzy C-means (FCM) has shown significant improvements in detecting malicious nodes in WSN. This method combines the soft clustering ability of FCM with the optimization power of HHO, creating a robust solution for identifying and isolating malicious nodes. Through the application of trust-based clustering, the proposed approach adapts to the dynamic behavior of the WSN, ensuring higher accuracy in malicious node detection and enhanced network performance. The proposed approach reduces packet loss significantly due to its ability to isolate malicious nodes early, improving routing efficiency and reducing packet drops. The high PDR in the proposed method indicates a more reliable and consistent packet transmission by minimizing interference from malicious nodes. With the optimization of clustering through HHO, the proposed approach achieves lower end-to-end delays by forming more efficient communication paths, minimizing delays in packet forwarding. Energy consumption is significantly reduced in the proposed approach due to more optimized routing, minimizing unnecessary energy usage, and prolonging network lifetime. The proposed approach achieves higher throughput due to its ability to

maintain more stable and efficient communication links by preventing malicious node interference.

References

Arab, A. (2023). The advanced wireless sensor networks' routing protocol to detect malicious nodes and behavior. *Journal of the Chinese Institute of Engineers*, 46(7), 805-812.

Debasis, K., Sharma, L. D., Bohat, V., & Bhadoria, R. S. (2023). An energy-efficient clustering algorithm for maximizing lifetime of wireless sensor networks using machine learning. *Mobile networks and applications*, 28(2), 853-867.

Faris, M., Mahmud, M. N., Salleh, M. F. M., & Alnoor, A. (2023). Wireless sensor network security: A recent review based on state-of-the-art works. *International Journal of Engineering Business Management*, 15, 18479790231157220.

Hassan, K., Madkour, M. A., & Nouh, S. A. (2023). A review of security challenges and solutions in wireless sensor networks. *Journal of Al-Azhar University Engineering Sector*, 18(69), 914-938.

Hu, H., Fan, X., & Wang, C. (2024). Efficient cluster-based routing protocol for wireless sensor networks by using collaborative-inspired Harris Hawk optimization and fuzzy logic. *Plos one*, 19(4), e0301470.

Liu, J., & Xu, F. (2023, April). Research on trust-based secure routing in wireless sensor networks. In Third International Conference on Artificial Intelligence and Computer Engineering (ICAICE 2022) (Vol. 12610, pp. 942-948). *SPIE*.

Mutar, M., & Hammood, D. A. (2023). A Systematic Study of Clustering Techniques for Energy Efficiency in Wireless Sensor Networks. *International Journal of Computing and Digital Systems*, 14(1), 1-1.

Mutar, M., & Hammood, D. A. (2023). A Systematic Study of Clustering Techniques for Energy Efficiency in Wireless Sensor Networks. *International Journal of Computing and Digital Systems*, 14(1), 1-1.

Panwar, A., & Nanda, S. J. (2023, December). Distributed Weighted Fuzzy C-Means Clustering for Wireless Sensor Network Data Analysis. In 2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 521-526). *IEEE*.

Sabitha, R., Prasad, C. G., & Karthik, S. (2023). Enhanced Security with Improved Defensive Routing Mechanism in Wireless Sensor Networks. *Computer Systems Science & Engineering*, 46(1).

Sikarwar, N., & Tomar, R. S. (2023). A Hybrid MFCM-PSO Approach for Tree-Based Multi-Hop Routing Using Modified Fuzzy C-Means in Wireless Sensor Network. *IEEE Access*, 11, 128745-128761.

Subedi, S., Acharya, S. K., Lee, J., & Lee, S. (2024, June). Two-Level Clustering Algorithm for Cluster Head Selection in Randomly Deployed Wireless Sensor Networks. In Telecom (Vol. 5, No. 3, pp. 522-536). *MDPI*.

Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. *Alexandria Engineering Journal*, 72, 37-50.

Wajgi, D. W., & Tembhurne, J. V. (2024). Localization in wireless sensor networks and wireless multimedia sensor networks using clustering techniques. *Multimedia Tools and Applications*, *83*(3), 6829-6879.

Wang, C., Liu, G., & Jiang, T. (2024). Malicious Node Detection in Wireless Weak-Link Sensor Networks Using Dynamic Trust Management. *IEEE Transactions on Mobile Computing*.

Xue, X., Shanmugam, R., Palanisamy, S., Khalaf, O. I., Selvaraj, D., & Abdulsahib, G. M. (2023). A hybrid cross layer with harris-hawk-optimization-based efficient routing for wireless sensor networks. *Symmetry*, *15*(2), 438.