Transactions on Soft Computing

www.tsc.reapress.com

Trans. Soft. Comput. Vol. 1, No. 2 (2025) 83–98.

Paper Type: Original Article

FL-GCN-LG-Trust: A Federated Graph-Based Trust Framework for Secure Cluster Optimization and Intrusion Detection in Underwater Wireless Sensor Networks

Kourosh Daniel Seifi[1], Parvaneh Asghari[1], Hamid Haj Seyyed Javadi[2,*], Mohammad Hadi Alaeiyan[3]

[1] Department of Computer Engineering, IAU, Science and Research Branch, Tehran, Iran; kourosh.seifi@iau.ir; asghari@iauctb.ac.ir.

[2] Department of Computer Engineering, Shahed University, Tehran, Iran; h.s.javadi@shahed.ac.ir.

[3] Department of Computer Engineering, K. N. Toosi University of Technology, Tehran, Iran; m.alaeiyan@kntu.ac.ir.

Citation:

Received: 10 July 2024 *Revised: 17 September 2024* *Accepted: 22 October 2024*	Daniel Seifi, K., Asghari, P., Haj Seyyed Javadi, H., & Alaeiyan, M. H. (2025). FL-GCN-LG-trust: A federated graph-based trust framework for secure cluster optimization and intrusion detection in underwater wireless sensor networks. *Transactions on Soft Computing*, 1(2), PP.

Abstract

This paper presents Federated Learning (FL)-Graph Convolutional Network (GCN)-Light Gradient (LG)-Trust, a federated, graph-based trust framework designed for anomaly detection and cluster optimization in Underwater Wireless Sensor Networks (UWSNs). The proposed architecture utilizes GCNs to compute both local and global trust scores, thereby improving the assessment of node reliability. By integrating FL, the framework facilitates collaborative training without centralizing data, thereby preserving privacy across distributed nodes. Additionally, a trust-aware cluster head selection protocol is developed to balance energy efficiency and network security. To evaluate its effectiveness, the framework is tested against traditional trust models under various attack scenarios, including data tampering, physical breaches, and environmental manipulations. Experimental results demonstrate that FL-GCN-LG-trust consistently outperforms existing models in detection accuracy, with significant improvements in true-positive rates and F1 Scores. Further simulations show that adjusting trust parameters and optimizing graph edge weights enhance system robustness while maintaining low communication overhead. The comparative analysis confirms that FL-GCN-LG-Trust not only provides improved detection performance but also offers scalable deployment in real-world underwater sensor networks. By combining FL techniques with trust modeling, the framework offers a secure, energy-efficient, and privacy-preserving solution for next-generation underwater network infrastructures.

Keywords: Underwater wireless sensor networks, Federated learning, Graph convolutional networks, Trust management, Attack detection.

1 | Introduction

Underwater Wireless Sensor Networks (UWSNs) have become an essential infrastructure for a variety of underwater applications, including oceanographic data collection, offshore resource exploration, climate

Corresponding Author: h.s.javadi@shahed.ac.ir

monitoring, and military surveillance systems [1], [2]. These networks generally consist of multiple sensor nodes deployed in underwater environments, interconnected through acoustic communication links. Each node is responsible for sensing, processing, and transmitting data to a central surface station or sink node for further analysis. A high-level overview of the UWSN architecture is shown in Fig. 1. Due to the challenging underwater environment, nodes often face limitations, including limited battery life, limited processing power, slow signal propagation, and bandwidth constraints [3]. These environmental challenges also make UWSNs more susceptible to various security threats. Malicious nodes may execute attacks such as selective forwarding, sinkhole, and Sybil attacks, thereby compromising network reliability [4]. Traditional centralized security solutions are often ineffective in this context due to communication latency, energy constraints, and the dynamic nature of underwater network topologies. As a result, there has been increasing research interest in developing lightweight, distributed, and context-aware solutions for trust management and attack detection [5]. One promising strategy to enhance the robustness of UWSNs involves implementing trust models that assess node behavior to identify and isolate malicious actors. Trust models can improve network resilience by enabling nodes to independently evaluate the trustworthiness of their peers based on local interactions.

However, existing trust models primarily focus on aggregating trust parameters globally, often neglecting local cluster behavior, resulting in less accurate trust assessments. Additionally, malicious behavior may influence neighboring nodes, further complicating trust estimation and attack detection. To overcome these limitations, this paper introduces FL-GCN-LG-Trust. This federated, graph-based trust model leverages Graph Convolutional Networks (GCNs) and Federated Learning (FL) to provide privacy-preserving, accurate, and energy-efficient attack detection and cluster optimization in UWSNs. The proposed approach models the UWSN as a graph, with nodes representing vertices and edges representing interactions. A GCN is utilized to learn both local and global topological features of the network, enabling the detection of subtle anomalies in node behavior. This information is integrated with a Light Gradient Boosting Machine (LGBM) model to improve detection accuracy further while maintaining low computational overhead. Moreover, FL enables distributed training of the GCN-LG-Trust model without sharing raw data across nodes, thereby safeguarding data privacy and reducing communication overhead. The key contributions of this paper are summarized as follows:

I. We propose a novel trust evaluation framework specifically designed for the clustered architecture of UWSNs. This model considers both node behavior and the structural roles within cluster-based environments.

II. We utilize GCNs to analyze network topology and identify potentially malicious node behavior via graph-structured trust propagation.

III. We incorporate LightGBM, a lightweight gradient boosting algorithm, to enable rapid, accurate classification of node trustworthiness, thereby reducing detection time and resource consumption.

IV. We integrate FL into the trust assessment framework to facilitate collaborative learning across distributed UWSN clusters while preserving the confidentiality of local data.

V. We evaluate the proposed approach through comprehensive simulations, demonstrating improvements in detection accuracy, energy efficiency, and clustering performance compared to traditional trust models.

The subsequent sections of this paper are organized as follows. Section 2 reviews related work on trust models and security in UWSNs. Section 3 describes the system model, including network, energy, and attack considerations. Section 4 details the design of the FL-GCN-LG-Trust framework. Section 5 presents the experimental setup, simulation results, and performance analysis. And finally, Section 6 offers concluding remarks and potential directions for future research.

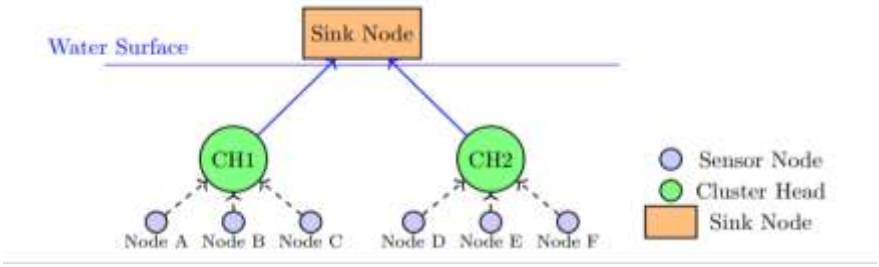

Fig. 1. Overview of a UWSN.

Sensor nodes transmit data to Cluster Heads (CHs) using acoustic communication. CHs forward aggregated data to a sink node at the surface. Nodes evaluate trust locally and globally within clusters.

2 | Related Work

As demand for secure and reliable UWSNs continues to grow, considerable research efforts have focused on improving trust management, attack detection, and network optimization. The existing body of literature can be broadly segmented into three main categories: trust modeling and management frameworks, optimization techniques for trust assessment, and the application of machine learning and deep learning methods for intelligent anomaly detection. In this section, we examine representative works within each category, discussing their significance and limitations within the context of underwater communication environments.

2.1 | Trust Algorithm and Management

Trust management in Wireless Sensor Networks (WSNs) and UWSNs has become a significant area of research due to resource limitations, adverse communication environments, and the presence of malicious nodes. Various approaches have been developed to enhance the security and reliability of these networks by implementing trust and reputation mechanisms. Initial strategies involved agent-based trust and reputation management systems, wherein dedicated agent nodes monitored trust metrics across the network to ensure secure operation while accommodating the limited processing and storage capabilities of sensor nodes [6]. Building on these foundations, lightweight, cluster-based trust management techniques have been proposed, leveraging hierarchical clustering to efficiently identify malicious nodes and reduce network overhead through localized trust assessments [7].

In underwater acoustic networks, characterized by constrained bandwidth and high latency, specialized trust models are necessary to comprehensively address link reliability, data integrity, and node behavior. Trust frameworks for Underwater Acoustic Signal Networks (UASNs) integrate multiple trust facets—such as link, data, and node trust—to better adapt to the underwater environment and improve the detection of malicious activities [8]. Additionally, trust models have been extended to monitor communication channels by employing statistical approaches, including Hidden Markov Models (HMM) combined with subjective logic frameworks, to identify potential attacks at the communication level [9]. In the underwater domain, these trust methodologies often incorporate both direct and indirect trust metrics, leveraging advanced optimization algorithms such as ant colony optimization to identify trustworthy routing paths while maintaining energy efficiency [10].

2.2 | Optimization of Trust Algorithms

Significant attention has been dedicated to optimizing trust algorithms to improve accuracy and resilience against malicious activity. The integration of cooperative filtering with fuzzy logic has been introduced to quantify node integrity, enabling networks to effectively identify and exclude dishonest or compromised nodes by analyzing collaborative behavior patterns [11]. To mitigate inaccuracies stemming from subjective weighting of trust metrics, trust assessment frameworks based on cloud theory have been proposed, thereby enhancing the robustness of trust evaluations in dynamic underwater network environments [12].

Additionally, dispute-resolution mechanisms have been developed to address conflicting trust assessments, thereby improving the reliability of trust management systems. These approaches often incorporate multiple performance indicators—such as communication delay, packet loss rate, and energy consumption—to provide a comprehensive evaluation of node trustworthiness [13].

2.3 | Machine Learning and Deep-Learning-Based Methods

Recent research has emphasized integrating machine learning and deep learning techniques to develop adaptive, intelligent trust models for UWSNs. Clustering algorithms, such as K-means, combined with classifiers, such as Support Vector Machines (SVMs), have been used to build trust evaluation frameworks that dynamically classify nodes based on behavioral trust metrics [14]. Reinforcement learning approaches have also been adopted to facilitate real-time updating of trust parameters, enabling the system to adapt effectively to evolving network conditions and emerging security threats [15]. More advanced predictive models incorporating Gaussian Mixture Models (GMM), HMM, and Long Short-Term Memory (LSTM) networks have been proposed to enhance routing protocols by accurately forecasting channel states and assessing node trustworthiness over time.

Furthermore, anomaly detection techniques leveraging isolation forest algorithms and environmental trust indicators have been introduced to strengthen the resilience of trust models against unforeseen or novel attacks. These models consider a combination of communication, data integrity, and energy consumption metrics to adaptively calibrate trust assessments in response to environmental dynamics. Additionally, adaptive trust frameworks based on LSTM neural networks have demonstrated improved ability to capture temporal dependencies in node behavior, thereby enhancing attack detection effectiveness. Spoofing attack detection has been addressed through node identification schemes that integrate time synchronization mechanisms with spatial wireless link correlation and clock skew analysis to accurately identify compromised nodes [16].

In the realm of security enhancements, innovative wireless key-generation methods tailored for IoT devices have been developed to mitigate replay attacks. These methods maintain the correlation in wireless channel measurements, reducing key discrepancy rates and bolstering communication security within underwater wireless networks [17]. To highlight the advancements of FL-GCN-LG-Trust, *Table 1* compares representative trust frameworks for UWSNs in terms of methodology, scalability, detection accuracy, and energy efficiency.

Table 1. Comparison of existing trust management models in UWSNs.

Reference	Methodology	Core Technique	Detection Accuracy	Energy Efficiency	Scalability	Privacy-Preserving
[6]	Agent-based trust	Monitoring agents	Medium	Medium	Low	No
[7]	Cluster-based trust	Hierarchical clustering	High	High	Medium	No
[8]	Hybrid trust model	Link + data + node trust	High	Medium	Medium	No
[14]	ML-based trust	SVM classification	Very high	Low	Medium	No
[15]	Reinforcement FL trust	Federated RL model	Very high	High	High	Yes
[17]	Decision Tree trust	Dynamic updating	High	High	Medium	Partial
Proposed FL-GCN-LG-Trust	Federated + GCN	Graph-based trust aggregation	Very high	High	High	Yes

3 | System Model

This section describes the system model employed in our proposed federated, graph-based trust framework, FL-GCN-LG-Trust, designed for attack detection and cluster optimization in UWSNs. The model encompasses the underwater network environment, energy consumption characteristics, and potential attack scenarios. These elements collectively serve as the basis for developing effective trust assessment and clustering strategies within underwater sensor networks. An abstract representation of the main components and information flows of our system model is illustrated in *Fig. 2*, providing a comprehensive visual context for the discussion that follows. Also, the procedural flows of the network model, energy computations, and adversarial simulations are detailed in *Algorithms 1-3*, providing a stepwise operational view of each core component before introducing our main federated trust algorithm.

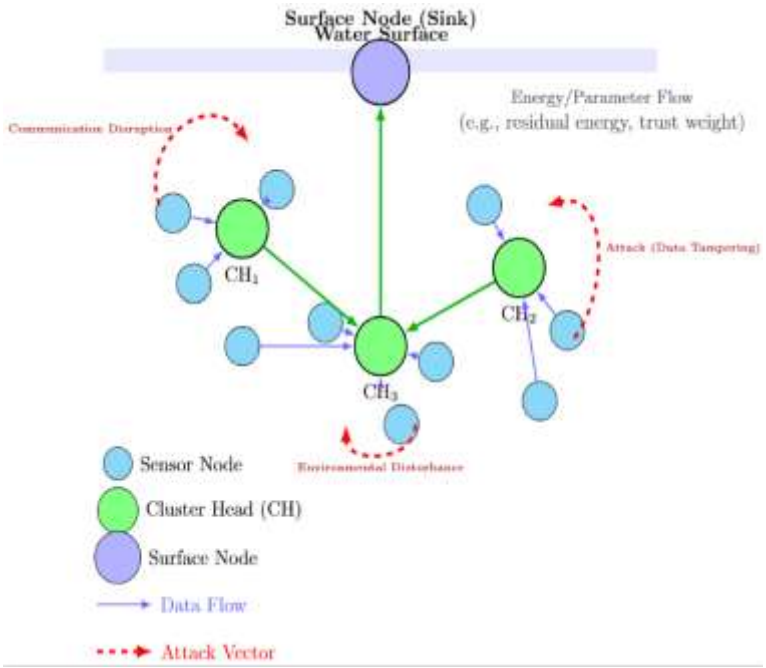

Fig. 2. Overview of the system model in FL-GCN-LG-trust.

3.1 | Network Model

The UWSN considered in this study is deployed within a three-dimensional cubic region. It includes a single Surface Node (SN) positioned at the center of the water surface and multiple sensor nodes (n) randomly distributed underwater. The SN serves as the data sink, collecting sensed data from underwater sensor nodes. It is assumed that the SN possesses ample storage capacity, computational resources, and an unlimited energy supply, ensuring continuous operation and effective data management [18].

All sensor nodes are homogeneous in hardware configuration, including storage, processing capability, and initial energy levels. Communication between nodes is facilitated via underwater acoustic signals within a specified transmission range R meters. The network operates in discrete iterations, each comprising two main phases: network initialization and data collection.

During the initialization phase, each node broadcasts signals to update its routing table and identify neighboring nodes, then transmits its status information to the SN. The SN employs a clustering algorithm to select suitable CH nodes, which subsequently notify their respective members. Member nodes join clusters by connecting to the nearest CH based on geographic proximity. During data collection, sensor nodes gather environmental data and forward it to their respective CHs. The CH nodes perform data aggregation and relay the processed data to the SN via multihop acoustic communication, enabling efficient underwater data

transmission [19]. The key parameters and characteristics of the sensor nodes and network communication are detailed in *Table 2*, providing an overview of the system setup used throughout this study.

Algorithm 1. UWSN initialization and clustering.

Require:
n underwater sensor nodes S = {s_1, s_2, …, s_n}, SN
Ensure:
Formed clusters with designated CHs and initialized data paths
Deploy SN at the center of the water surface.
Randomly deploy n sensor nodes within the 3D underwater environment.
For each iteration:
a. Initialization Phase:
- Each sensor node broadcasts discovery beacons and updates its routing table.
- Each node identifies neighboring nodes based on signal strength and distance.
- Each node transmits status information (e.g., residual energy, location) to SN.
- SN applies clustering algorithm (e.g., LEACH or GCN-based) to select CHs.
- Selected CHs broadcast cluster invitation messages to nearby nodes.
- Each node joins the nearest CH based on proximity and signal quality.
b. Data Collection Phase:
- Member nodes collect environmental data (e.g., temperature, pressure).
- Each member node transmits sensed data to its respective CH.
- Each CH aggregates received data and forwards it to the SN via a multihop relay.

Table 2. System model parameters and descriptions.

Parameter	Description	Unit
n	Number of underwater sensor nodes	-
SN	Surface node	-
R	Communication range of nodes	meters (m)
P_sen	Power for data sensing	Watts (W)
γ	Energy discount rate for sensing and receiving	-
P_0	Power of successful data transmission	Watts (W)
A(d)	Energy attenuation function over distance d	-
P_rec	Power of successful data reception	Watts (W)
P_agg	Power consumption for data aggregation	Watts (W)
n_packet	Packet length	bits
CH	Cluster Head node	-

3.2|Energy Consumption Model

Energy efficiency is a vital consideration in UWSNs, given the limited battery capacity of underwater nodes and the substantial energy requirements of acoustic communication. Our model accounts for four primary energy consumption types in sensor nodes: data collection, data transmission, data reception, and data aggregation.

I. Data collection energy: sensor nodes consume energy during the sensing process to gather environmental data from underwater regions. The sensing power and the size of the collected data packets influence this energy expenditure. In secure network configurations, the energy related to data collection is considered negligible [20].

II. Data transmission energy: Underwater data transmission requires considerable energy due to signal attenuation and the unique characteristics of acoustic channels. Energy consumption increases with higher transmission frequencies and longer distances. Acoustic signals in water experience significant attenuation, and high-frequency or long-distance transmissions result in notable energy losses and signal distortion [21].

III. Data reception energy: Receiving data also consumes energy; however, in this model, the energy used by sensor nodes during data reception is not explicitly accounted for. Energy costs are proportional to the volume of data received and to environmental factors affecting communication quality [22].

IV. Data aggregation energy: CHs nodes incur additional energy costs when aggregating data from multiple cluster members. The total energy consumed for data aggregation depends on the number of member nodes and the size of their data packets [23].

Algorithm 2. Energy consumption computation in UWSN.

Require:
Network topology with all sensor nodes and their initial energy levels
Ensure:
Updated residual energy for each node after data collection and transmission
For each sensor node i, initialize residual energy E_i.
Compute energy for data collection:
$E_{col} = P_{sen} \times t_{col}$ (if significant).
For each data transmission:
a. Calculate distance to receiver d.
b. Compute transmission energy:
$E_{tx} = P_0 \times A(d) \times t_{tx}$.
For each received packet:
Compute reception energy:
$E_{rec} = P_{rec} \times t_{rec}$.
For CHs:
Aggregate data energy consumption:
$E_{agg} = P_{agg} \times DataSize$.
Update residual energy:
For each node, update
$E_i = E_i - (E_{col} + E_{tx} + E_{rec} + E_{agg})$.

3.3 | Attack Model

The underwater environment is susceptible to various types of attacks that can compromise network functionality and data integrity. Our system model considers three primary attack scenarios to simulate potential adversarial impacts on UWSNs:

I. Data tampering attacks: malicious entities infiltrate the network to intercept and modify sensor data. The compromised data is transmitted to the sink node via typical routing paths, undermining the authenticity and reliability of the collected information. Such attacks can lead to discrepancies between data from compromised nodes and that of legitimate neighboring nodes, thereby adversely affecting data-dependent applications [24].

II. Communication disruption attacks: adversaries may employ techniques such as electromagnetic pulses, noise injection, and flooding to interfere with the physical communication channels of underwater nodes. These tactics result in unstable connections, increased energy consumption, and reduced network reliability, ultimately shortening the system's overall operational lifetime.

III. Environmental attacks: environmental factors such as water currents, temperature fluctuations, and physical obstacles contribute to unstable network conditions. The model assumes these effects manifest as localized, range-limited disturbances centered at specific points, with their influence diminishing radially. Nodes within these affected areas may experience decreased sensing accuracy, reduced energy efficiency, and impaired channel stability [25].

These attack models guide the development of our trust evaluation and cluster optimization strategies by emulating realistic underwater threats, thereby enhancing the network's resilience against both malicious activities and environmental disruptions.

Algorithm 3. Attack scenario simulation in UWSN.

Require:
Deployed UWSN topology, set of possible attack types
Ensure:
Updated system status, trust levels, and performance metrics after simulated attacks
For each attack round, randomly select targeted nodes or areas within the UWSN.
Apply selected attack type:
a. Data tampering:
- Intercept or alter transmitted data packets.
- Relay modified data to the SN with falsified values.
b. Communication Disruption:
- Inject noise, interference, or flooding packets into communication links.
- Mark affected links as unstable.
- Increase the energy consumption of targeted nodes due to retransmissions.
c. Environmental Attack:
- Simulate local environmental disturbances (e.g., fluctuating temperature or water currents).
- Degrade node sensing accuracy and channel reliability within the affected region.
Adjust overall system status, routing decisions, and trust calculations according to the observed effects of the simulated attacks.

4 | Problem Formulation

In UWSNs, ensuring secure and efficient communication poses unique challenges due to the distinctive characteristics of the underwater environment. Factors such as limited bandwidth, high latency, and restricted energy resources complicate network design and operation. Additionally, the presence of malicious or malfunctioning nodes introduces security risks that can adversely affect network performance and data integrity. To address these challenges, it is imperative to develop a comprehensive framework that integrates trust evaluation with energy-aware mechanisms. This section details the network model, trust assessment methodologies, and cluster-formation strategies that, together, establish a robust and secure architecture for an underwater sensor network.

4.1 | Network Model and Assumptions

The proposed UWSN consists of a set of sensor nodes $S = \{s_1, s_2, \ldots, s_n\}$ randomly deployed in a three-dimensional underwater volume to sense environmental parameters. Communication is primarily acoustic-based, constrained by high propagation delay and low data rates [26]. Each node s_i possesses limited energy E_i, and the initial energy allocation is represented as:

$$E_i(0) = E_0, \text{for all} i \in S. \quad (1)$$

The energy consumption for a transmission over distance d_{ij} from node s_i to s_j is modeled as:

$$E_{tx}(i,j) = P_t \times A(d_{ij}) \times t_{tx}, \quad (2)$$

where P_t is the transmission power, $A(d_{ij})$ is the acoustic attenuation function, and t_{tx} is the transmission duration. The energy model also includes reception and data aggregation costs:

$$E_{rec}(i) = P_{rec} \times t_{rec}, E_{agg}(i) = P_{agg} \times D_i, \quad (3)$$

where D_i is the size of the aggregated data at the node s_i. To enhance scalability and reduce energy waste, nodes form clusters, each managed by a CHs. CHs handle data aggregation and forward compressed data to

the SN. The hierarchical structure minimizes long-range communication and extends overall network lifetime [12].

It is assumed that:

I. Nodes can monitor residual energy and track direct neighbors.

II. Some nodes may be malicious and engage in packet dropping or data falsification.

III. Nodes can perform periodic trust updates to detect and isolate malicious nodes [27].

Nodes with residual energy E_i below a predefined threshold E_{th} are excluded from CH selection:

$$E_i < E_{th} \Longrightarrow s_i \text{ not eligible for the CH role.} \quad (4)$$

These assumptions guide the design of an energy-aware and trust-driven clustering model tailored for UWSNs [28].

4.2 | Trust Evaluation in the Network

Trust evaluation in UWSNs quantifies the reliability and behavioral consistency of nodes to mitigate risks from compromised or malfunctioning entities. Each node s_i maintains a trust score T_i based on both direct and indirect observations [22]. The direct trust component derives from observed packet forwarding behavior:

$$T_i^{dir} = \frac{P_{success}(i)}{P_{total}(i)}, \quad (5)$$

where $P_{success}(i)$ and $P_{total}(i)$ denote the number of successfully forwarded packets and total packets transmitted through the node s_i, respectively. The indirect trust component aggregates recommendations from neighboring nodes N_i:

$$T_i^{ind} = \frac{1}{|N_i|} \sum_{j \in N_i} T_j(i). \quad (6)$$

The composite trust score is then expressed as:

$$T_i = \alpha \times T_i^{dir} + (1 - \alpha) \times T_i^{ind}, \quad (7)$$

where $\alpha \in [0,1]$ balances the weight between firsthand experience and neighbor feedback [15]. Nodes whose trust value drops below the predefined threshold T_{th} are considered unreliable and excluded from routing or CHs candidacy:

$$T_i < T_{th} \Longrightarrow s_i \text{ is untrustworthy.} \quad (7)$$

The trust evaluation is dynamically updated at regular intervals:

$$T_i(t+1) = (1 - \lambda) T_i(t) + \lambda \times T_i^{new}, \quad (8)$$

Where λ controls the sensitivity to recent observations [14]. To ensure sustainable operation, trust is coupled with energy levels in the Trust-Energy Composite Metric (TEC):

$$TEC_i = \beta \times T_i + (1 - \beta) \times \frac{E_i}{E_0}, \quad (7)$$

Where β determines the trade-off between trust reliability and energy availability [8].

Nodes with higher TEC_i values are prioritized for essential roles such as CH selection or relay participation, optimizing both security and longevity.

Table 3 presents a comparative analysis of trust evaluation methodologies in UWSNs, highlighting key metrics including detection accuracy, energy efficiency, computational complexity, and scalability. A comprehensive understanding of these trade-offs is vital to developing optimized trust management frameworks that effectively balance security assurances with the resource limitations inherent to underwater sensor deployments.

Table 3. Performance comparison of trust evaluation methods in UWSNs.

Trust Method	Detection Accuracy	Energy Consumption	Computational Complexity	Scalability	Remarks
Direct trust	Medium	Low	Low	Moderate	Relies on direct interactions
Indirect trust	High	Medium	Medium	High	Uses recommendations from neighbors
Bayesian trust model	High	Medium	High	Moderate	Incorporates uncertainty
Fuzzy logic trust	Medium	Low	Medium	High	Handles imprecise data well
Machine learning based trust	Very High	High	Very High	High	Adaptive but resource-intensive

4.3 | Cluster Formation and Optimization

Clustering aims to structure the network for efficient communication and energy utilization. The CHselection process prioritizes nodes based on trustworthiness and residual energy [26]. Let the CH eligibility score for the node s_i be defined as:

$$CH_i = \gamma \times T_i + (1 - \gamma) \times \frac{E_i}{E_0}, \quad (11)$$

where $\gamma \in [0,1]$ controls the weighting between trust and energy factors. Nodes broadcast their T_i and E_i values to neighboring nodes. The node with the highest CH_i within a neighborhood radius R is elected as the CHs:

$$CH_i = \max_{s_j \in N_i} (CH_j). \quad (12)$$

Once clusters form, CHs aggregate data and forward the aggregated information to the SN. The total energy consumption per CH during an aggregation cycle is expressed as

$$E_{CH} = n_c \times (E_{tx} + E_{rec}) + E_{agg}, \quad (13)$$

where n_c is the number of member nodes in the cluster. To maintain stability, the network periodically re-evaluates trust and energy levels. If a CH's residual energy drops below E_{th}or its trust score T_i declines below T_{th}, re-clustering is triggered:

$$(E_i < E_{th}) \vee (T_i < T_{th}) \implies \text{Re-clustering event.} \quad (14)$$

This adaptive re-optimization ensures continuous resilience against energy depletion, malicious activities, and environmental variations [12], [27], [28].

Fig. 3 illustrates the trust- and energy-aware CH selection process, highlighting the dynamic relationship between network security, efficiency, and survivability.

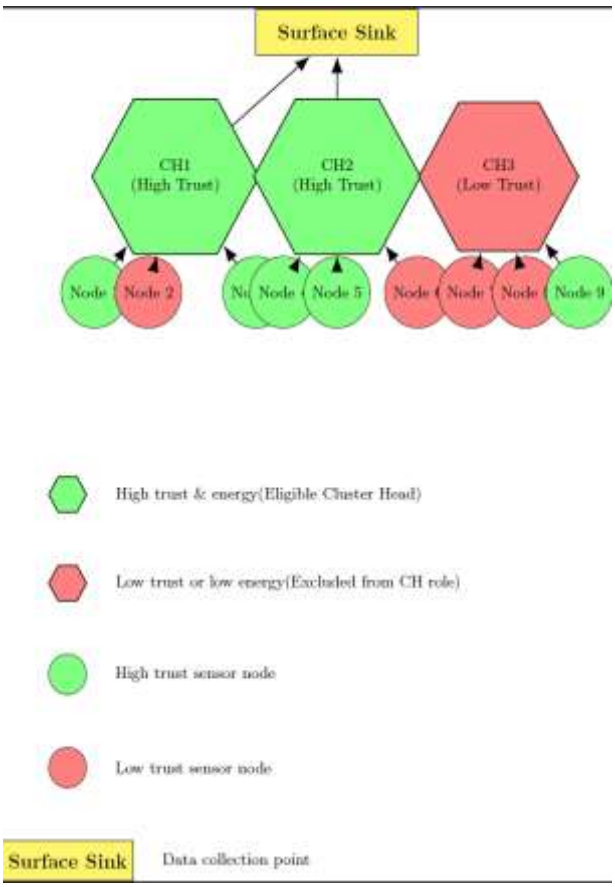

Fig. 3. Trust-based cluster head selection process in UWSNs.

5 | Experimental Results and Analysis

This section delineates the experimental framework, including simulation parameters and dataset preparation protocols, and provides a comprehensive evaluation of the proposed trust model's efficacy in detecting malicious behavior in UWSNs. The methodology entails detailing the setup of the simulation environment, the generation of datasets, and the assessment of multiple trust-evidence aggregation algorithms. Subsequently, the performance of the GCNs combined with the LightGBM GCN-LG model is benchmarked against alternative classification algorithms, focusing on metrics such as detection accuracy, memory footprint, and computational complexity. Lastly, a sensitivity analysis is conducted to examine the influence of key hyperparameters on detection performance, facilitating the identification of optimal parameter configurations.

5.1 | Parameters and Dataset of Simulation Experiment

In this study, the training dataset for the trust model was generated using MATLAB R2023b. Trust parameter aggregation was implemented using the PyTorch Geometric library, while training and inference were executed in Python. The simulation environment was hosted on a system featuring an Intel Core i7-13700HX processor (13th Generation), an NVIDIA GeForce 4060 Ti GPU, and 16 GB of RAM. A total of 100 sensor nodes were randomly deployed within a three-dimensional underwater space measuring 300 m × 300 m × 300 m, with the sink node positioned centrally at the upper surface. The network was assumed to be static, with no node mobility considerations. The simulation parameters are detailed in *Table 3*. Dataset generation involved 500 distinct node deployment configurations, each comprising 100 iterative rounds that simulated network initialization, cluster formation via the HEED algorithm, and data transmission. Malicious attack events were randomly initiated at various rounds, targeting randomly selected nodes, as referenced in [29], [30].

5.2 | Comparison of Trust Evidence's Algorithms

The performance of the proposed trust evidence computation approach was evaluated in underwater clustered networks and benchmarked against conventional energy-based trust, communication trust, and data trust algorithms. Trust evidence metrics were generated for each algorithm under identical network configurations. These trust parameters served as input features for training a Random Forest (RF) classifier aimed at attack detection. As demonstrated in *Fig. 4*, the proposed method consistently surpassed traditional algorithms across a range of attacked node densities. Detection efficacy declined with increasing attack density, attributable to increased feature ambiguity between benign and compromised nodes [31].

A detailed evaluation of targeted attack vectors revealed that the proposed algorithm achieved superior detection efficacy against data tampering attacks, as illustrated in Fig. 5, resulting in higher true positive rates. Additionally, it maintained a detection accuracy exceeding 80% in physical attack scenarios, whereas conventional techniques frequently exhibited accuracy below 30%. Regarding environmental manipulation attacks, the algorithm consistently maintained a detection accuracy of 75% to 93%, significantly surpassing that of traditional methods, which typically achieved an accuracy below 60% [32].

5.3 | Comparison of Trust Model

Using a dataset comprising 300 network simulation scenarios under three distinct attack vectors, we assessed the performance of our GCN-LG model, which integrates edge weights derived from communication delay metrics and signal strength indicators. The GCN-LG approach was benchmarked against the Receiver Operating Characteristic (ROC), Spatial-Temporal Monitoring System (STMS), and LSTM methodologies, with evaluation based on F1-score. *Figs. 3* and *4* illustrate that the GCN-LG model attains statistically significantly higher F1-scores across all considered attack types, reflecting enhanced attack detection efficacy. Notably, the F1-score for physical attack detection plateaus beyond an attack density threshold of 20%, whereas other models exhibit precipitous declines in performance. Furthermore, the GCN-LG maintains an F1-score exceeding 85% against environmental attack scenarios, thereby demonstrating its robustness and effectiveness in safeguarding underwater sensor network operations [33].

5.4 | Comparison of Model Memory Usage and Calculation Time

Considering the dynamic underwater environment and limited computational resources, we quantitatively evaluated memory consumption and processing latency for various trust models that employ identical trust-evidence aggregation algorithms. The LightGBM and STMS models exhibited peak memory utilization below 35 MiB, whereas RF and LSTM models required approximately 94 MiB and 116.6 MiB, respectively. The proposed GCN-LG model demonstrated a memory footprint of 62.7 MiB, effectively balancing classification accuracy and resource efficiency. Processing durations for traditional machine learning approaches ranged from 5 to 10 seconds; deep learning models exceeded 20 seconds, while LightGBM-based models completed inference in under 2 seconds. The hybrid GCN-LightGBM trust framework processed the input data in approximately 12.6 seconds, indicating its viability for real-time implementation in underwater network scenarios [34].

5.5 | Confidence Model Parameter Configuration

Table 4 additionally quantifies the effect of varying the edge data weight (communication delay weight) on the GCN-LG model's F1-score. Optimal detection performance was observed when the edge data weight was set to 45%-80% across varying attack densities. Moreover, the table elucidates the correlation between the number of leaf nodes in the model and detection efficacy. An optimal leaf node count near 39 maintains a balance between classification accuracy and computational resource utilization, mitigating the overhead associated with increased leaf node quantities, as outlined in [35].

Table 4. Impact of communication delay, leaf node weight, and the number of leaf nodes on GCN-LG model detection performance and computational resource consumption.

Parameter	Values Tested	Effect on GCN-LG Model Performance
Edge data weight (communication delay weight)	0%, 15%, 30%, 45%, 60%, 80%, 100%	Best F1-score achieved when the weight is between 45% and 80%, indicating optimal detection performance in this range across various attack densities.
Number of leaf nodes in the model	20, 30, 39, 45	A leaf node count of around 39 provides a good balance between detection accuracy and computational efficiency, avoiding the overhead of larger counts.

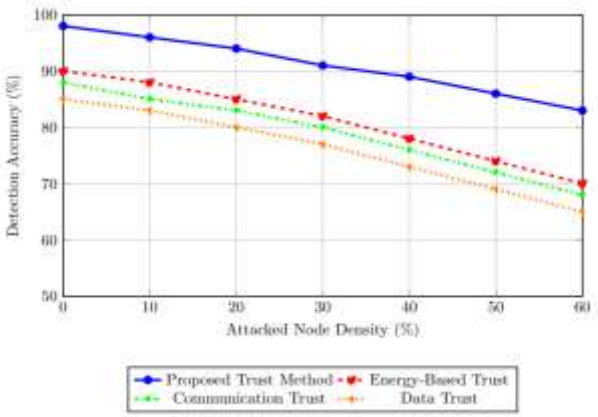

Fig. 4. Detection accuracy comparison of the proposed trust algorithm versus traditional algorithms under varying attacked node densities.

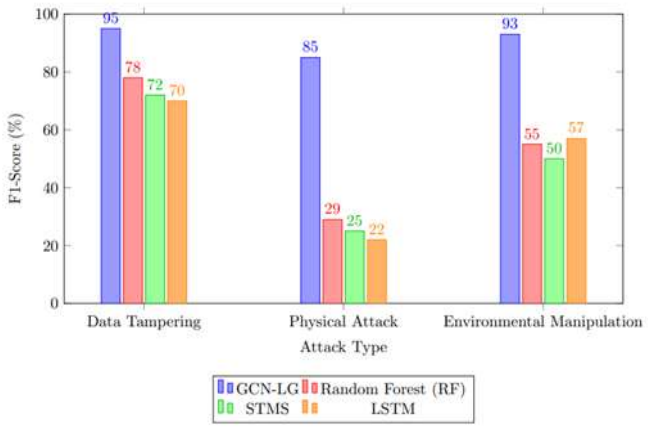

Fig. 5. F1-score comparison of GCN-LG model against RF, STMS, and LSTM models for data tampering, physical, and environmental manipulation attacks.

6 | Conclusion

This study introduces FL-GCN-LG-Trust, a federated, graph-based trust framework tailored for secure cluster optimization and intrusion detection within UWSNs. The model synergistically integrates local and global trust evidence with energy-efficient CHs selection algorithms to enhance both communication security and network performance. Employing FL facilitates privacy-preserving training processes while significantly reducing communication overhead, a critical consideration in underwater communication environments.

Experimental results indicate that FL-GCN-LG-Trust surpasses conventional trust assessment algorithms in detecting a range of adversarial behaviors, including data tampering and physical node compromises. As illustrated in *Figs. 4* and *5*, the model maintains consistently high detection accuracy across varying attack intensities. Parameter-optimization analyses reveal that optimal trust performance hinges on the calibration of communication-delay weighting factors and the number of leaf nodes in the network topology, as detailed in *Table 3*.

Future work focuses on integrating blockchain technology and adaptive learning mechanisms to enhance system robustness and support real-time operational capabilities. Overall, FL-GCN-LG-Trust provides a scalable, intelligent trust management solution suited for clustered UWSNs.

References

[1] Akyildiz, I. F., Pompili, D., & Melodia, T. (2005). Underwater acoustic sensor networks: Research challenges. *Ad hoc networks*, *3*(3), 257–279. https://doi.org/10.1016/j.adhoc.2005.01.004

[2] Tian, W., Zhao, Y., Hou, R., Dong, M., Ota, K., Zeng, D., & Zhang, J. (2023). A centralized control-based clustering scheme for energy efficiency in underwater acoustic sensor networks. *IEEE transactions on green communications and networking*, *7*(2), 668–679. https://doi.org/10.1109/TGCN.2023.3249208

[3] Riveros-Rojas, G. J., Cespedes-Sanchez, P. P., Pinto-Roa, D. P., & Legal-Ayala, H. (2024). Energy-and-blocking-aware routing and device assignment in software-defined networking—a MILP and genetic algorithm approach. *Mathematical and computational applications*, *29*(2), 18. https://doi.org/10.3390/mca29020018

[4] Zhu, R., Boukerche, A., Long, L., & Yang, Q. (2024). Design guidelines on trust management for underwater wireless sensor networks. *IEEE communications surveys & tutorials*, *26*(4), 2547–2576. https://doi.org/10.1109/COMST.2024.3389728

[5] Sreekantha, B., & Shaila, K. (2024). Exploring the synergy of machine learning algorithms in wireless sensor networks: A comprehensive survey. *Intelligent electrical systems and industrial automation* (pp. 45–57). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-6806-6_4

[6] Al-Shamaileh, M., Anthony, P., & Charters, S. (2024). Agent-based trust and reputation model in smart IoT environments. *Technologies*, *12*(11), 208. https://doi.org/10.3390/technologies12110208

[7] Babu, G. R., Vaishali, K., Madhuri, K. H., Deepika, E., & Chowdary, K. K. (2024). Trusted net: A lightweight cluster-based trust sensing system for IoT networks. *Journal of science & technology*, *9*(4), 74–83. https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

[8] Jiang, B., Zhou, R., Luo, F., Cui, X., Liu, Y., & Song, H. (2024). Hybrid trust model for identifying malicious attacks in underwater acoustic sensor network. *IEEE sensors journal*, *24*(16), 26743–26754. https://doi.org/10.1109/JSEN.2024.3424252

[9] Lenard, T., Collen, A., Benyahya, M., Nijdam, N. A., & Genge, B. (2023). Exploring trust modeling and management techniques in the context of distributed wireless networks: A literature review. *IEEE access*, *11*, 106803–106832. https://doi.org/10.1109/ACCESS.2023.3320945

[10] Zhu, R., Boukerche, A., & Yang, Q. (2023). Towards a trusted channel energy-aware routing algorithm for underwater sensor networks. *Proceedings of the 19th ACM international symposium on QOS and security for wireless and mobile networks* (pp. 47–51). New York, NY, USA: Association for computing machinery. https://doi.org/10.1145/3616391.3622777

[11] Liao, H. (2025). E-commerce live-streaming platform and decision support system based on fuzzy association rule mining. *International journal of computational intelligence systems*, *18*(1), 41. https://doi.org/10.1007/s44196-025-00744-4

[12] Zhu, R., Boukerche, A., Feng, L., & Yang, Q. (2023). A trust management-based secure routing protocol with AUV-aided path repairing for underwater acoustic sensor networks. *Ad hoc networks*, *149*, 103212. https://doi.org/10.1016/j.adhoc.2023.103212

[13] Jiang, Z., Xing, F., Tan, Y., & Tong, F. (2024). A discrete-time markov chains cloud-based trust management approach model for underwater wireless sensor networks. *2024 international conference on*

artificial intelligence of things and systems (AIOTSYS) (pp. 1–7). IEEE. https://doi.org/10.1109/AIoTSys63104.2024.10780741

[14] Liu, C., Ye, J., An, F., & Jiang, W. (2024). An adaptive trust evaluation model for detecting abnormal nodes in underwater acoustic sensor networks. *Sensors*, *24*(9), 2880. https://doi.org/10.3390/s24092880

[15] He, Y., Han, G., Li, A., Taleb, T., Wang, C., & Yu, H. (2023). A federated deep reinforcement learning-based trust model in underwater acoustic sensor networks. *IEEE transactions on mobile computing*, *23*(5), 5150–5161. https://doi.org/10.1109/TMC.2023.3301825

[16] Kalghatgi, H., Dhawle, M., & Raut, U. (2023). Defense techniques against spoofing attacks in wireless sensor networks. *Materials today: Proceedings*. https://doi.org/10.1016/j.matpr.2023.03.357

[17] Huan, X., Miao, K., Chen, W., Jia, P., & Hu, H. (2024). Kerra: An internet of things wireless key generation resistant to replay attacks. *IEEE internet of things journal*, *11*(17), 29035–29048. https://doi.org/10.1109/JIOT.2024.3406702

[18] Yan, J., Guan, X., Yang, X., Chen, C., & Luo, X. (2025). A survey on integration design of localization, communication and control for underwater acoustic sensor networks. *IEEE internet of things journal*, *12*(6), 6300–6324. https://doi.org/10.1109/JIOT.2025.3525482

[19] Campagnaro, F., Steinmetz, F., & Renner, B. C. (2023). Survey on low-cost underwater sensor networks: from niche applications to everyday use. *Journal of marine science and engineering*, *11*(1), 125. https://doi.org/10.3390/jmse11010125

[20] Zayed, M. M., Shokair, M., Ghallab, R., & others. (2025). Modeling and analysis of underwater optical wireless communication channels. *International journal of engineering and applied sciences-october 6 university*, *2*(1), 32–45. https://doi.org/10.21608/ijeasou.2025.349270.1040

[21] Theocharidis, T., & Kavallieratou, E. (2025). Underwater communication technologies: A review. *Telecommunication systems*, *88*(2), 54. https://doi.org/10.1007/s11235-025-01279-x

[22] Shah, S., Munir, A., Salam, A., Ullah, F., Amin, F., AlSalman, H., & Javeed, Q. (2024). A dynamic trust evaluation and update model using advance decision tree for underwater wireless sensor networks. *Scientific reports*, *14*(1), 22393. https://doi.org/10.1038/s41598-024-72775-4

[23] Jain, S., & Verma, R. K. (2024). A taxonomy and survey on grid-based routing protocols designed for wireless sensor networks. *ACM computing surveys*, *56*(8), 1–41. https://doi.org/10.1145/3653315

[24] Zhang, M., Feng, R., Zhang, H., & Su, Y. (2023). A recommendation management defense mechanism based on trust model in underwater acoustic sensor networks. *Future generation computer systems*, *145*, 466–477. https://doi.org/10.1016/j.future.2023.03.043

[25] Gupta, S., & Singh, N. P. (2024). Underwater wireless sensor networks: A review of routing protocols, taxonomy, and future directions. *The journal of supercomputing*, *80*(4), 5163–5196. https://doi.org/10.1007/s11227-023-05646-w

[26] Bharany, S., Sharma, S., Alsharabi, N., Tag Eldin, E., & Ghamry, N. A. (2023). Energy-efficient clustering protocol for underwater wireless sensor networks using optimized glowworm swarm optimization. *Frontiers in marine science*, *10*, 1117787. https://doi.org/10.3389/fmars.2023.1117787

[27] Zukarnain, Z. A., Amodu, O. A., Wenting, C., & Bukar, U. A. (2023). A survey of Sybil attack countermeasures in underwater sensor and acoustic networks. *IEEE access*, *11*, 64518–64543. https://doi.org/10.1109/ACCESS.2023.3288330

[28] Khan, M. U., Otero, P., & Aamir, M. (2024). An energy efficient clustering routing protocol based on arithmetic progression for underwater acoustic sensor networks. *IEEE sensors journal*, *24*(5), 6964–6975. https://doi.org/10.1109/JSEN.2024.3354252

[29] Kanavalli, A., Chaudhari, S. S., & others. (2024). Trust-based data fusion and machine learning for underwater sensor networks. *2024 4th Asian conference on innovation in technology (Asiancon)* (pp. 1–6). IEEE. https://doi.org/10.1109/ASIANCON62057.2024.10838202

[30] Uyan, O. G., Akbas, A., & Gungor, V. C. (2023). Machine learning approaches for underwater sensor network parameter prediction. *Ad hoc networks*, *144*, 103139. https://doi.org/10.1016/j.adhoc.2023.103139

[31] Rakesh, S., Praveen, R. V. S., Ramkumar Prabhu, M., Chauhan, A., Pal, S., & Kalra, G. (2024). *Graph convolutional neural networks for attack detection in wireless sensor networks security*. https://dx.doi.org/10.2139/ssrn.5091230

[32] Tiwari, A., & Darbari, M. (2025). *Emerging trends in computer science and its application*. CRC Press Boca Raton, FL, USA. https://dx.doi.org/10.1201/9781003606635

[33] Kumar, M., Goyal, N., Qaisi, R. M. A., Najim, M., & Gupta, S. K. (2025). Joint trust-based detection and signature-based authentication technique for secure localization in underwater wireless sensor network. *Multimedia tools and applications*, *84*(31), 37845–37864. https://doi.org/10.1007/s11042-025-20683-8

[34] Mir, M., & Trik, M. (2025). A novel intrusion detection framework for industrial IoT: GCN-GRU architecture optimized with ant colony optimization. *Computers and electrical engineering*, *126*, 110541. https://doi.org/10.1016/j.compeleceng.2025.110541

[35] Le, M., Hoang, D. T., Nguyen, D. N., Pham, Q. V., & Hwang, W. J. (2023). Wirelessly powered federated learning networks: Joint power transfer, data sensing, model training, and resource allocation. *IEEE internet of things journal*, *11*(21), 34093–34107. https://doi.org/10.1109/JIOT.2023.3324151