International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 15 Issue 04 Year 2023

Steiner Whisper Clustering and Gated Recurrent Trust-Based Secure Routing for Underwater Sensor Networks

O. Vidhya*
Research Scholar (FT), Department of Computer Science, Rathnavel Subramaniam College of Arts and Science(Autonomous), Sulur, Coimbatore, Tamil Nadu, India.
o.vidhya17@gmail.com
S. Ranjitha Kumari
Associate Professor, Rathnavel Subramaniam College of Arts and Science (Autonomous), Sulur, Coimbatore, Tamil Nadu, India
ranjithakumari@rvsgroup.com

Article History

Received: 10 November 2023
Revised: 12 December 2023
Accepted: 25 January 2024

Abstract

Underwater Wireless Sensor Networks (UWSNs) have prompted the growing curiosity of several researchers in industrial establishments, surveillance, trading, and academic purposes over the past few years. In recent days, the application of UWSNs in different areas of application has seen a monumental advancement. In UWSN, several techniques are developed by clustering as well as deep learning for optimizing the problem of secure data routing. In this work, an energy-efficient method called Steiner Chinese Whisper Clustering and Memory Gated Recurrent Trust-based (SCWC-MGRT) secured routing in UWSN is proposed. The energy-efficient SCWC-MGRT method for secured routing in UWSN is split into two sections: clustering and secured routing. Initially, based on the energy level, underwater sensor nodes are grouped by employing the Steiner Chinese Whisper Node Clustering model. Here, the energy consumption model is designed separately for node initialization and data forwarding using the Steiner Triangulation function. Finally, maximum residual energy and distance were utilized to choose the cluster head. Then, secured data routing with underwater sensors is carried out by means of a memory-centered gated recurrent trust-based secure routing model. By the memory-centred nature, specified underwater sensor node for current time stamp and hidden state of previous time stamp, validation is through and therefore secured routing is secured. The NS2 platform was utilized to simulate SCWC-MGRT and compare the two other routing methods. SCWC-MGRT method of outcomes appreciably enhances energy efficiency, data confidentiality rate, and delivery ratio without forfeiting too much end-to-end delay.

Keywords: Under Water Sensor Networks, Steiner Triangulation, Chinese Whisper Node, Clustering, Memory Centered, Gated Recurrent

1. Introduction

Secure UWSNs has received a great deal over the past few days. Security susceptibility has persistently been the most used by malicious users for both political and financial advantages. Extensive types of attacks are said to prevail, ranging from network sniffing to disrupting entire operations. Routing techniques are revealed for different types of attacks. These types of attacks are said to have a profound negative influence on the routing completely.

An enhanced cluster setup as well as reduced energy utilization was provided in [1] during cluster setup, a novel Energy Efficient Circular Spinning (EECS) clustering method to network lifetime. The proposed EECS method proposed to system performance by reducing the Cluster Head (CH) selection phase or cluster setup phase and, finally, the minimum energy consumption of networks. Nevertheless, it failed to focus on depth-based routing protocols and to reduce the energy usage in re-clustering or cluster setup. Resilience against depth spoofing was considered [2] by the energy-efficient depth-based probabilistic routing protocol (DPR). The proposed DPR protocol efficiently resists depth-spoofing attacks with a reasonably efficient energy overhead. But, the packet delivery ratio was better.

An in-depth summarization of data gathering in UWSN basis of routing was discussed in [3]. Reinforcement learning was discussed in [4] by the routing protocol. Several energy-efficient routing mechanisms were discussed in [5]. As far as the ocean in several countries is concerned, two major factors to be focused on in monitoring the underwater environment are economic development and border security. Data gathering methods were analyzed in [6]. However, the network's lifespan was not enhanced.

Total energy and residual energy as fitness functions while deriving the clustering protocol for UWSN included in [7] with optimized glowworm swarm optimization. Nevertheless, the network overhead incurred during clustering was not focused. To address this aspect, cluster heads and sub-cluster head nodes were designed [8], but they also reduced the packet loss rate considerably.

Two key problems addressed: (1) How to ensure energy-efficient routing with distance factor taken into consideration. (2) The problem of ensuring secure data routing is handled. Contributions have been given by,

To propose energy-efficient Steiner Chinese Whisper Clustering and Memory Gated Recurrent Trust-based (SCWC-MGRT) secured routing in UWSN, split into two sections, one for clustering and the second for ensuring secured routing.

The Steiner Chinese Whisper Node Clustering algorithm is provided to reduce energy consumption as well as the delay involved in both clustering and cluster head selection. By applying the Steiner Triangulation function, one can quickly search for optimal CHs, therefore reducing energy consumption. Also, by applying Chinese Whisper Node Clustering, significant cluster formation is ensured, therefore forming an optimal cluster.

To design a centred Gated Recurrent-based secure routing algorithm that measures distance trust and mobility trust separately and then applies a centred Gated Recurrent model, therefore improving data confidentiality significantly.

SCWC-MGRT secured routing in UWSN outcome can significantly balance energy consumption as well as less delay with improved delivery ratio and data confidentiality. Compared with EECS and DPR, the SCWC-MGRT method outperforms 10% and 29% in terms of node energy consumption, end-to-end delay up to 22%, 35%, 8%, 19% in terms of data confidentiality as well as packet delivery ratio by 8%, 15%.

The article has been planned based on the modern state of the art presented in Section 2. A detailed description of the proposed SCWC-MGRT secured routing method is included in Section 3. Simulation and performance evaluation metrics are analyzed in Section 4. Section 5 displays the results. The conclusion is demonstrated in Section 6.

2. Related Works

The one-Leap Fuzzy-based Clustering Technique (OLFCT) was proposed in [9] that not only alleviated the exhaustion rate but K-means and ant colony optimization-based routing (KACO) was investigated in [10] with the objective of minimizing energy consumption. However, the delay was not decreased.

Throughput was improved, and secured data transmission was ensured in [11] with deep reinforcement-based extreme learning machines (DRLELM). Vampire nodes were classified [12] by means of a Dual Encoding Recurrent Neural network (DERNNet). Best relay nodes were made in [13] with the DL-high dynamic biased track method. However, they are also not free from attacks. Self-learning potentiality was enhanced with strong generality using a new DL basis of link prediction method [14].

Network lifetimes were developed in [15] employing adaptive Deep Q-Network-basis of energy as well as a latency-aware routing protocol. The advantage of broadcast nature was considered [16] with a combined relay two-hop cooperative communication algorithm. A secure routing protocol was introduced in [17] to address the vulnerability.

In [18], Secure Energy Efficient and Cooperative routing protocols were presented. With the purpose of identifying as well as mitigating attacks, the distributed mechanism was presented in [19]. Ttrust strategy-based dynamic Bayesian game (TSDBG) was designed in [20]. Here, a secure site was initially constructed, following which trust and payoff factors were measured via communication to obtain specific nodes.

2.1 Problem Definition

The Steiner Chinese Whisper Clustering and Memory Gated Recurrent Trust-based (SCWC-MGRT) method secured routing in UWSN proposed to improve energy efficiency. The energy consumption and delay were minimized by both clustering and cluster head selection in the Steiner Chinese Whisper Node Clustering algorithm. The data confidentiality is significantly improved by the memory-centred gated Recurrent trust-based secure routing algorithm, which measures distance trust and mobility trust separately. The depth-based routing protocols were not focused on reducing energy usage. Data gathering methods were analyzed by reducing the network's lifespan.

3. Methodology

The proposed SCWC-MGRT secured routing method comprises two main phases: clustering and secured data routing with high data confidentiality. Initially, underwater sensor nodes are considered as input for performing secured data routing or routing. With the proposed method split into two sections, for clustering UWSNs, Steiner Chinese Whisper Node Clustering is carried out in the SCWC-MGRT method.

3.1 Architecture of Underwater Sensor Network

In the targeted volume ‘i*j*k’ of UWSNs, let us assume a network situation comprising UWSNs and sink nodes (i.e., surface sink and the onshore sink). This network is referred to by a set of underwater sensors that are dispersed in an even fashion with notable locations spread over three-dimensional areas and are responsible for secure communication. Each UWSN observes data as well as stores it during their buffer. Figure 1 shows the structure of the underwater sensor network.

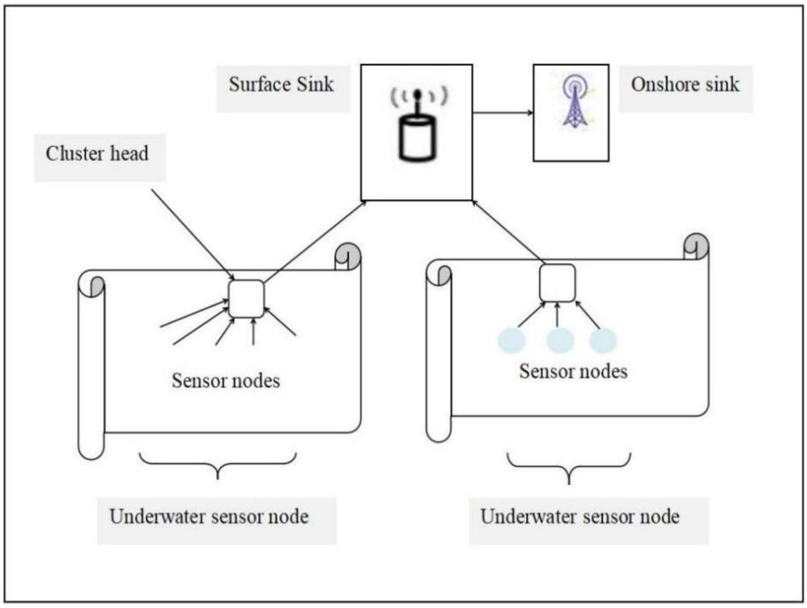

Figure 1. Structure of Steiner Chinese Whisper Node Clustering

As illustrated in the above figure, let '$G = (V, E)$' be a weighted graph with underwater sensor nodes '$\{USN_1, USN_2, \ldots, USN_n\} \in V$' and weighted edges '$\{USN_1, USN_j, W_{ij}\} \in E$' with weight '$W_{ij}$ respectively. In topology, due to detail, underwater sensors are portable because the water current's velocity changes are found to be very swift. The sink node function is located at a ceaseless speed at the shore, which gathers the data packet and forwards related to the data packet toward the sink node. The sink node plays an essential role in minimizing the propagation latency/delay and energy consumption of UWSN. In this work, the first cluster formation is modelled in an energy-efficient manner that is administered by the cluster heads.

3.2 Steiner Chinese Whisper Node Clustering

This section presents a Steiner Time Linear Chinese whispers model for clustering to gather optimization actions of links. Moreover, the transmission power of the sender node is fine-tunable, i.e., for communication to take place between shorter distances, the communication power is reduced to circumvent or keep away from the other underwater sensor nodes' intervention and also to minimize energy consumption. The cluster formation in this work is modelled, taking into consideration the Steiner point wherein the objective remains in associating the input points by minimum total length. With this, UWSNS grouped based on total energy consumption, therefore significantly reducing delay. Figure 2 shows the Steiner Chinese Whisper Node Clustering model structure.

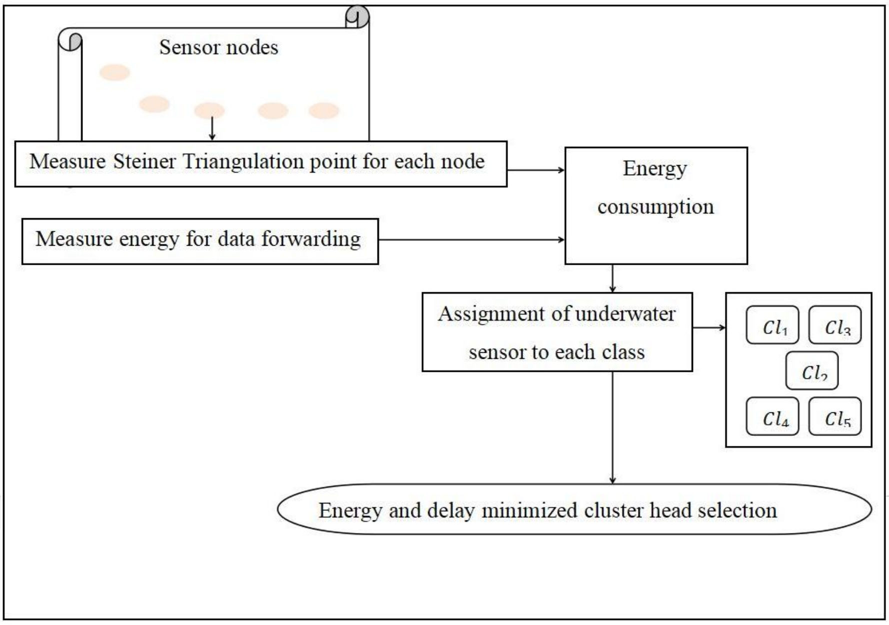
Sensor nodes
Measure Steiner Triangulation point for each node
Energy consumption
Measure energy for data forwarding
Assignment of underwater sensor to each class
Cl_1
Cl_3
Cl_2
Cl_4
Cl_5
Energy and delay minimized cluster head selection

Figure 2. Structure of Steiner Chinese Whisper Node Clustering Model

As illustrated in the above figure, the Steiner Chinese Whisper Node Clustering groups UWSN based on the highest residual energy and distance factors. First, by employing the Steiner Triangulation function, energy consumption is measured. The cluster was formed by grouping UWSNs using Chinese Whisper Node Clustering via energy. Residual energy, as well as distance factor, are employed to perform cluster head selection. Using this model, the UWSNs can manage their networks better owing to the fact that Chinese is immensely high speed even if the number of UWSNs and links is very high in the network. In this manner, a better solution (i.e., optimal clustering) is said to be arrived at.

By using packet size '$\mathrm{DP_{size}}$', let us assume that only 'n' underwater sensor nodes distribute their positional data for transmission or reception. The least energy consumed for UWSN in receiving each bit signal has '$\mathrm{LEC^{i}_{Trans}}$' with the distance between sensors being '$\mathrm{Dis_{(USN_i,USN_j)}}$', and the energy consumed in identifying Steiner Triangulation point to all node on time 't' is formulated as given below.

$$\mathrm{SPEC^{t}_{i}} = \begin{cases} \mathrm{EC^{i}_{Rec} + EC^{i}_{Trans}} \\ \mathrm{EC^{i}_{Rec} = DP_{size} + LEC^{i}_{Rec}} \\ \mathrm{EC^{i}_{Trans} = DP_{size} * \left(EC^{i}_{Rec} + LEC^{i}_{Trans} * Dis_{(USN_i,USN_j)}\right)} \end{cases} \quad (1)$$

From the above equation (1), '$\mathrm{EC^{i}_{Rec}}$'has Steiner Triangulation point determined with energy consumption for reception of data packets, energy consumption for transmission of data packets '$\mathrm{EC^{i}_{Trans}}$', along with the data packet size '$\mathrm{DP_{size}}$' and the energy consumed for an underwater sensor node in sending per bit signals '$\mathrm{LEC^{i}_{Trans}}$' respectively. With the further assumption that the '$\mathrm{(USN_i, USN_j, USN_k)}$' are adjoining or neighbouring UWSNas well as transmitting of variable packet size '$\mathrm{DP_{size}}$' for transmission or reception onshore sink node. Through data packet received at underwater sink node '$\mathrm{DP^{t}_{USN}}$', energy requested to forward data packet at a time 't' is evaluated as given below.

$$\mathrm{DPFEC^{t}_{i}} = \begin{cases} \mathrm{EC^{i}_{Rec} + EC^{i}_{Trans}} \\ \mathrm{EC^{i}_{Rec} = LEC^{i}_{Rec} * DP^{t}_{USN}} \\ \mathrm{EC^{i}_{Trans} = \left(EC^{i}_{Rec} + LEC^{i}_{Trans} * Dis_{(USN_i,USN_j)}\right) * DP^{t}_{USN}} \end{cases} \quad (2)$$

Finally, with the above two equations (1) and (2), on time instance 't', every sum of energy consumption underwater sensor '$\mathrm{USN_i}$' has mathematically stated by:

$$\mathrm{EC(USN^{t}_{i}) = SPEC^{t}_{i} + DPFEC^{t}_{i}} \quad (3)$$

Cluster is formulated by Steiner point for each node. Next, the cluster head selection is performed in our work by means of Steiner Chinese Whisper Node Clustering. The Chinese Whisper Node Clustering objective in our work remains to identify groups of underwater sensor nodes that broadcast the same data packet to their adjacent nodes. First, a different class, $'\mathrm{Cl}'$, is assigned to each vertex $'\mathrm{USN_i} \in \mathrm{V_i}'$ and generates cluster '$\mathrm{C_i}$'. Next, with the objective of combining the iterations, a series of rounds is performed. At each round, each vertex or the underwater sensor node is analyzed in an arbitrary fashion and allocates its majority class among those related by its adjacent nodes. To be more specific, vertex or underwater sensor node $'\mathrm{USN_i}'$ is assigned to class 'Cl', '$\{\mathrm{USN_i}, \mathrm{USN_j}\}$' has higher total edges weights where 'Cl' has a class of $'\mathrm{USN_i}'$. It has a mathematical formula expressed below.

$$\mathrm{Cl(v)} = \mathrm{argmax} \sum_{\{\mathrm{USN_i}, \mathrm{USN_j}\} \in \mathrm{G}} \mathrm{EC}(\mathrm{USN_i^t}), \mathrm{EC}(\mathrm{USN_j^t}) \quad (4)$$

With the clustering process stopping as well as outputs final clustering, no sooner iteration creates no modification. Finally, with obtained clusters, via highest adjacent node residual energy $'\mathrm{RES(AN)}'$, distance between current node, adjacent node '$\mathrm{Dis(CN, AN)}$' and hop count as of adjacent node for underwater sink node '$\mathrm{HC(AN, US)}$' respectively, cluster head is formed.

$$\mathrm{CH} = \frac{\mathrm{RES(AN)}}{\mathrm{Dis(CN,AN)} * \mathrm{HC(AN,US)}} \quad (5)$$

$$\mathrm{Dis(CN, AN)} = \sqrt{\left(\mathrm{USN_i(AN)} - \mathrm{USN_i(AN)}\right)^2 + \left(\mathrm{USN_j(CN)} - \mathrm{USN_j(CN)}\right)^2} \quad (6)$$

From the above equations (5) and (6), $'\mathrm{CH}'$ has a cluster head node chosen by taking into consideration the distance factor $'\mathrm{Dis(CN, AN)}'$. Also, by disabling unused nodes, energy consumption is reduced, and lifetime is enhanced. A pseudo-code representation of Steiner Chinese Whisper Node Clustering is given below.

Algorithm 1. Steiner Chinese Whisper Node Clustering

```
Input: underwater sensor nodes '$USN = \{USN_1, USN_2, ..., USN_n\}$', underwater sink node '$US = \{US_1, U S_2, ..., US_s\}$', water surface base station '$BS$'
Output: Energy and delay-minimized cluster head
Step 1: Initialize '$n$', '$s$', time instance '$t$'
Step 2: Begin
Step 3: For each underwater sensor node '$USN$' in '$V$' with underwater sink node '$US$' and water surface base station '$BS$'
    //Steiner triangulation
    Step 4: Measure energy consumed in identifying the Steiner point for each node at a time '$t$' as given in (1)
    Step 5: Measure energy consumed to forward the data packet at a time '$t$' as given in (2)
    Step 6: Evaluate the total energy consumption of each underwater sensor '$USN_i$' at time instance '$t$' as given in (3)
    //Chinese Whisper Node Clustering – cluster formation
    Step 7: Maximize the sum of weights of the edges of each underwater sensor node and assign it to class '$Cl$' as given in (4)
Step 8: **Measure** distance as given in (5) and (6)
Step 9: **Return** cluster head ‘$CH$’
Step 10: **End for**
Step 11: **End**
```

As given in the above algorithm, the energy consumption model using the Steiner point is measured separately for both node initialization and data forwarding via the Steiner Triangulation function. Next, the total energy consumed is measured for a specific time instance. Following this, each UWSN is assigned for class in such a manner, therefore forming a cluster via Chinese Whisper Node Clustering. Finally, the highest residual energy, as well as distance, picks the cluster head.

3.3 Memory Centered Gated Recurrent Trust based Secure Routing

Despite anonymity ensured by means of encryption, however, they are found to be high both in terms of energy consumption and processing costs. Over the past few years, trust-based models have been found to be better at detecting malicious underwater sensor nodes and, therefore, ensuring secured data routing in UWSN. In this section, a novel memory-centered gated recurrent Trust-based secure routing is designed. By generating a trust relationship between underwater sensor nodes using the fitness function, security services can be ensured. Using fitness function, taking into consideration of UWSNtrust values based on distance and mobility, secured routing is said to be ensured in UWSNs. Finally, an optimal route path between source and sink is generated for secured communication in UWSN. Figure 3 shows the structure of memory-centered gated recurrent trust-based secure routing in UWSN employed in our work for secured routing.

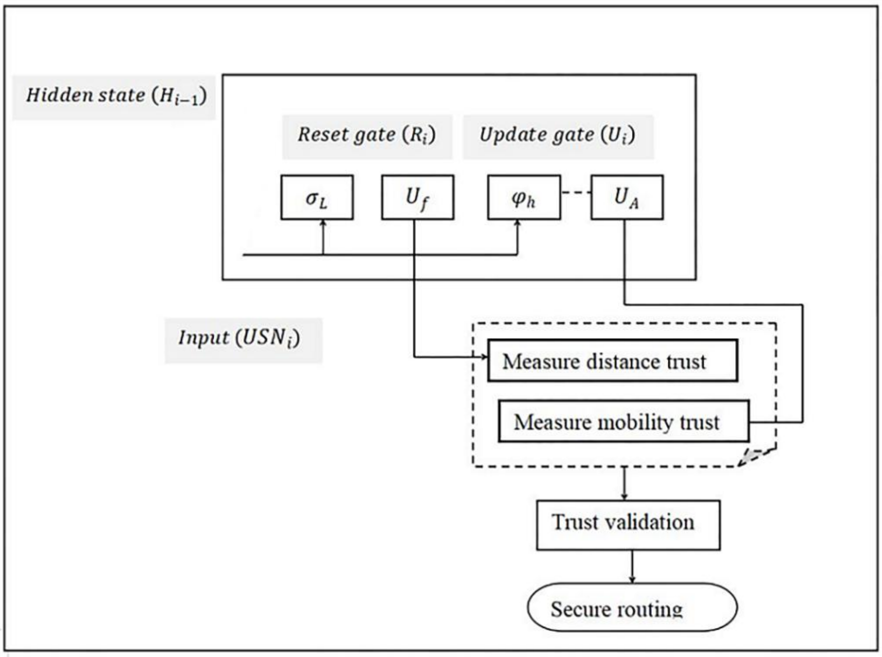

Figure 3. Structure of Memory-Centered Gated Recurrent Trust-based Secure Routing

As shown in the above figure, the memory-centered gated recurrent trust-based secure routing is split into two stages. In the first stage, trust evaluation, i.e., distance trust and mobility trust, is made, following which, in the second stage, secure routing is ensured via the Memory Centered Gated Recurrent model. In transmission range 'TR’ and is represented as ‘$\mathrm{Trust_{Dis}}$, distance trust refers to the distance among 'CH’ as well as underwater sink nodes ‘US'. The underwater sink node 'US’ in UWSN is positioned at the surface of the sea to acquire corresponding data from the respective underwater sensor nodes. ‘TR' of some cluster head node '$\mathrm{CH(a, b, c)}$' is the potentiality to communicate the data packet. Therefore, qualified CHs are 'QCH', and all 'CHs' that comprise 'TR' are denoted as 'QCH', which is mathematically represented below.

$$\mathrm{QCH_k = k \in \ US_i \Lambda Dis_{CH}^{US} \leq TR} \tag{7}$$

From the above equation (7), '$\mathrm{US_i}$' represents the underwater sink node in UWSN, the distance among cluster head node '$\mathrm{k(a_k, b_k, c_k)}$' has '$\mathrm{Dis_{CH}^{US}}$', as well as underwater sink node '$\mathrm{US_i(a_k, b_k, c_k)}$' respectively. Higher is trust and vice versa; the value of '$\mathrm{QCH_k}$' lies amid '0' as well as '1', maximum results. Then, the underwater sensor node distance trust is mathematically formulated as given below.

$$\mathrm{Trust_{Dis}} = \sqrt{(\mathrm{a_k - a_i})^2 + (\mathrm{b_k - b_i})^2 + (\mathrm{c_k - c_i})^2} \tag{8}$$

In addition to the distance trust, mobility trust is also evaluated. The underwater sensor node mobility trust is formulated as given below.

$$\mathrm{Trust_{mobility}} = \sqrt{\mathrm{CH_V^2 + USN_V^2 - 2CH_V^2 USN_V^2 \cos\left(\frac{CH_\theta - USN_\theta}{2}\right)}} \tag{9}$$

From the above equation (9), mobility trust '$\mathrm{Trust_{mobility}}$' results are obtained based on the velocity of cluster head '$\mathrm{CH_V^2}$', velocity of underwater sensor node '$\mathrm{USN_V^2}$', the angular displacement of the cluster head '$\mathrm{CH_\theta}$' as well as '$\mathrm{USN_\theta}$' has an angular displacement of USN respectively. The mobility trust of underwater sensor nodes ranges between '0' and '1'; the lower the resultant values, the better the selection for routing and vice versa. Finally, a holistic trust is obtained based on both the distance trust and mobility trust, as given below.

$$\mathrm{TTrust} = \mathrm{Trust_{Dis}} + \mathrm{Trust_{mobility}} \tag{10}$$

The whole trust of each CH is evaluated through important inputs. This is performed using a memory-centered gated recurrent unit. The three main blocks of a centred Gated Recurrent Unit are the forget gate, the activation gate and the actual output gate. This is formulated as given below.

$$\mathrm{f_i} = \sigma_{\mathrm{L}}(\mathrm{W_f USN_i + U_f O_{i-1} + B_f}) \tag{11}$$

$$\mathrm{A_i} = \varphi_{\mathrm{h}}(\mathrm{W_A USN_i + U_A(f_i \odot O_{i-1}) + B_h}) \tag{12}$$

$$\mathrm{O_i} = (1 - \mathrm{f_i}) \odot \mathrm{O_{i-1}} + \mathrm{f_i} \odot \mathrm{A_i} \tag{13}$$

From the above equation (11), the forget vector '$\mathrm{f_i}$' for '$\mathrm{i-th}$' underwater sensor node is arrived at via a logistic function 'σ_{L}' for the corresponding underwater sensor node '$\mathrm{USN_i}$' with an output vector '$\mathrm{O_{i-1}}$' and the bias vector '$\mathrm{B_f}$' respectively. By triggering the '$\mathrm{U_f}$' function, underwater sensor node distance trust is measured. In a similar manner, the equation in (12) returns the activation vector '$\mathrm{A_i}$' for the '$\mathrm{i-th}$' underwater sensor node via hyperbolic tangent function 'φ_{h}' for the corresponding underwater sensor node '$\mathrm{USN_i}$' with an output vector '$\mathrm{O_{i-1}}$' and the bias vector '$\mathrm{B_h}$'. By triggering the '$\mathrm{U_A}$' function, underwater sensor node mobility trust is measured. Also, as the information is retained over a period of time, it is also referred to as the Memory Centered Gated Recurrent Unit. Both the distance trust value and mobility trust value are retained over a period of time, therefore improving the data confidentiality rate and data delivery ratio to a greater extent. Finally, the total trust value 'TTrust' is compared with the output in the Memory Centered Gated Recurrent Unit '$\mathrm{O_i}$' to validate. Upon successful validation, secured routing is established; otherwise, proceed with another set of information. By higher data confidentiality, secured data routing between underwater sensor nodes has been attained. A memory-centered gated recurrent Trust-based secure routing algorithm is given below.

Algorithm 2. Memory Centered Gated Recurrent Trust-based Secure Routing

```
Input: underwater sensor nodes '$USN = \{USN_1, USN_2, ..., USN_n\}$', underwater sink node '$US = \{US_1, U S_2, ..., US_s\}$', water surface base station '$BS$'

Output: Secured routing

Step 1: Initialize '$n$', '$s$', time instance '$t$'
Step 2: Initialize '$B_f = 1$', '$B_h = 1$'
Step 3: Begin
Step 4: **For** each underwater sensor node '$USN$' in '$V$' with underwater sink node '$US$', water surface base station '$BS$' and cluster head '$CH$'
//**Trust evaluation**
Step 5: Formulate qualified CHs as in (7)
Step 6: Evaluate underwater sensor node distance trust as in (8)
Step 7: Evaluate underwater sensor node mobility trust as in (9)
Step 8: Evaluate total trust value as in (10)
// **Memory Centered Gated Recurrent Unit**
Step 9: Formulate forget gate as in (11)
Step 10: Formulate the activation gate as in (12)
Step 11: Obtain output gate value as in (13)
Step 12: **If** the output gate value '$O_i$' is equal to '$TTrust$'
    Step 13: **Then** proceed with secure communication between underwater sensor nodes '$USN$'
Step 14: **End if**
Step 15: **If** output gate value '$O_i$' is not equal to '$TTrust$'
    Step 16: **Then** do not proceed with communication between underwater sensor nodes '$USN$'
    Step 17: **Go to** step 4
Step 18: **End if**
Step 19: **End for**
Step 20: **End**
```

As given in the above algorithm, with the objective of improving the data confidentiality rate and packet delivery ratio, the trust evaluation function is applied to evaluate the trust based on distance and mobility. Following this, the trust and non-trust underwater sensor nodes are stored in the gated recurrent unit. Here, by triggering the functions separately for distance and mobility, validation is made. Moreover, memory-centered optimization methods utilized to transfer data privacy across UWSN have arrived at. As the advantage of the algorithm being memory centred given UWSN of the current time stamp as well as the hidden state of the previous time stamp according to the evaluated trust and stored in the lookup table, validation is made. Upon successful validation, communication between underwater sensor nodes is said to take place securely. On the contrary, upon unsuccessful validation, no communication is said to be established between underwater sensor nodes.

4. Performance Analysis and Experiments Results

Experimental evaluation is carried out in SCWC-MGRT secured routing in UWSN on different factors based on the number of underwater sensor nodes as well as the number of data packets. A performance analysis of the proposed method has been compared with the existing EECS [1] and DPR [2] for UWSN, as discussed. It is implemented on the NS2 simulator. For this experiment, at an examination region of 500×500 m^2, 50, 100, ..., 500 underwater sensor nodes are arranged in a dynamic fashion. The simulation settings used for this experiment are listed in Table 1.

Table 1. Simulation Parameters

S. No.	Parameters	Description
1	Size of the region	500 m * 500 m
2	Number of underwater sensor nodes	50, 100, 150, 200, 250, 300, 350, 400, 450, 500
3	Number of the sink node	1
4	Maximum transmission radius (m)	87
5	Propagation delay (S)	0.00066
6	Transmission time (S)	2.9
7	Node initial energy (J)	5
8	Data packet size	250 Bytes
9	Control message size	250 Bytes
10	Communication range	200 m
11	Minimum communication range	125 m
12	Maximum communication range	150 m
13	Initial energy	1J
14	Simulation time	100 s
15	Simulation runs	10

5. Simulation Results

We compared the proposed SCWC-MGRT secured routing in UWSN with that of EECS [1] and DPR [2]. The comparisons are conducted with total energy consumption, data confidentiality rate, end-to-end delay, and packet delivery ratio. Performance metrics are defined as follows.

5.1 Energy Consumption

Owing to the reason that all underwater sensor nodes were energy-constrained, the significance of measuring energy efficiency is extremely high in UWSNs. The proposed method took into consideration the energy measurement. It is defined as the whole energy needed by each underwater sensor node, together with the energy consumption of nodes in sending, receiving as well and inert states.

$$EC = \sum_{i=1}^{n} USN_i * EC\ (Sensing\ single\ USN\ ) \qquad (14)$$

From the above equation (14), energy consumption ‘ EC ' is measured by taking into consideration the network samples 'USN_i’ involved in the simulation process and the time consumed in sensing single node ‘$EC\ (Sensing\ single\ USN\ )$’. It is measured in terms of joules (J).

Table 2. Tabulation for Energy Consumption using SCWC-MGRT, EECS [1] and DPR [2]

Underwater Sensor Nodes	Energy Consumption (J)		
	SCWC-MGRT	EECS	DPR

50	600	700	850
100	685	755	935
150	725	820	1025
200	850	985	1145
250	935	1055	1325
300	1025	1105	1455
350	1135	1215	1635
400	1245	1345	1805
450	1385	1455	1935
500	1425	1585	2055

Total energy consumption based on underwater nodes ranges between 50 and 500, as shown in Table 2. The proposed SCWC-MGRT method consumes less energy than the [1] and [2] method. This is because the SCWC-MGRT method chooses the best energy-efficient nodes to forward data packets by including energy consumption during cluster formation. In contrast, in the SCWC-MGRT method, the candidate nodes for clustering formation are selected based on the Steiner Triangulation point. This, in turn, reduces the energy consumption using the SCWC-MGRT method by 10% compared to [1] and 29% compared to [2], respectively.

5.2 End-to-End Delay

End-to-end delay is a significant parameter to consider. It measured for effectively received data packets on the destination end. It refers to the average required data packet transmission as a source to any of the sinks.

$$Delay_{EE} = \sum_{i=1}^{n} USN_i * \{[t_{act}] - [t_{ex}]\} \qquad (15)$$

From the above equation (15), '$Delay_{EE}$' has the end-to-end delay, number of network samples 'USN_i' involved in the simulation, and 't_{act}' has a difference among actual time needed as well as expected time of consumption 't_{ex}' respectively. These are estimated in milliseconds (ms).

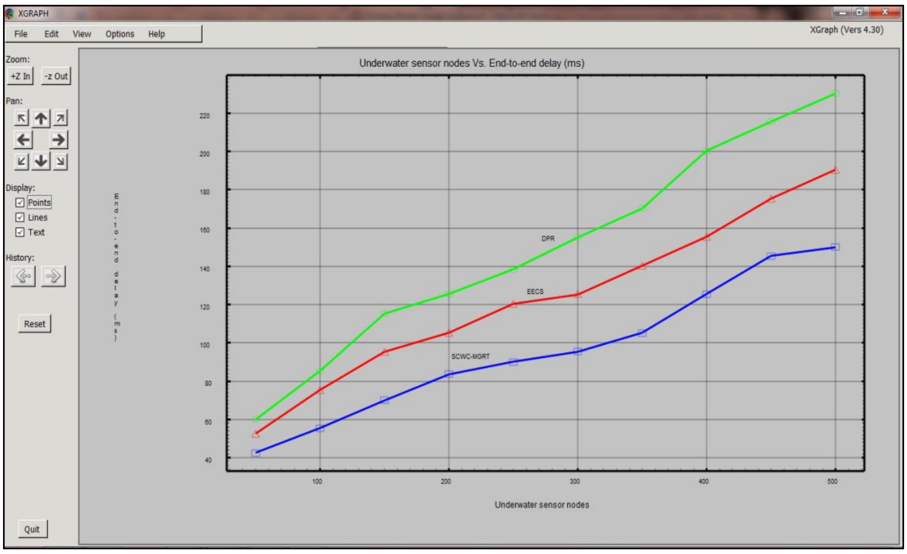

Figure 4. Graphical Representation of End-to-End Delay

The average end-to-end delay is displayed in Figure 4. SCWC-MGRT method of Average end-to-end delay is shorter compared to [1] and [2], mainly because unused nodes are disabled during the cluster head selection process. Chinese Whisper Node Clustering uses a proposed method to identify the global optimal next hop. Our method utilizes the Steiner Triangulation point for organized forwarding of candidate UWSNs that all unused nodes do not participate in the cluster head selection process, thus minimizing the end-to-end delay using the SCWC-MGRT method by 22% compared to [1] and 35% compared to [2].

5.3 Data Confidentiality Rate

The next parameter of significance is the data confidentiality rate while ensuring secured data routing in UWSN. It evaluated the percentage of data packets that are received by authorized receivers.

$$C_{Rate} = \sum_{i=1}^{m} \frac{S_{ID}}{S_i} * 100 \qquad (16)$$

From the above equation (16), the data confidentiality rate 'C_{Rate}' is measured based on the device's data received by the intended recipient device 'S_{ID}', a whole number of device samples transmitted with the source device as input 'S_i' for simulation. These are computed in percentage (%).

Table 3. Tabulation for Data Confidentiality using SCWC-MGRT, EECS [1] and DPR [2]

Underwater sensor nodes	**Data confidentiality rate (%)**		
	SCWC-MGRT	EECS	DPR
50	94	88	84
100	92.15	84.35	83.25
150	90	84	78
200	89.35	83.55	76.35
250	88	82	75
300	87.45	81.25	72.15
350	86	79	70
400	85.35	78	69.45
450	84	77.35	67
500	83.15	76	65.25

Table 3 above illustrates the graphical representation of the data confidentiality rate. The fitness function of every UWSN, based on distance as well as mobility, improves the device's data received by the intended recipient device, which effectively improves the data confidentiality rate. What is more, its underwater sensor node distance trust and underwater sensor node mobility trust based on eligible cluster head ensures eligible device data to be received by the intended recipient, resulting in higher data confidentiality improvement by 8% as well as 19% than [1] and [2] respectively.

5.4 Packet Delivery Ratio

It is referred to as the proportion of data packets effectively received with sinks DP_{ds}. This metric demonstrates the flexibility of the solution under distinct traffic intensity. The packet delivery ratio is mathematically expressed as given below.

$$PDR = \sum_{i=1}^{m} \frac{DP_{ds}}{DP_i} * 100 \qquad (17)$$

Where 'PDR' has a data packet delivery ratio and 'DP_i' has a number of data packets sent at specific time instances, respectively. These are calculated in percentage (%).

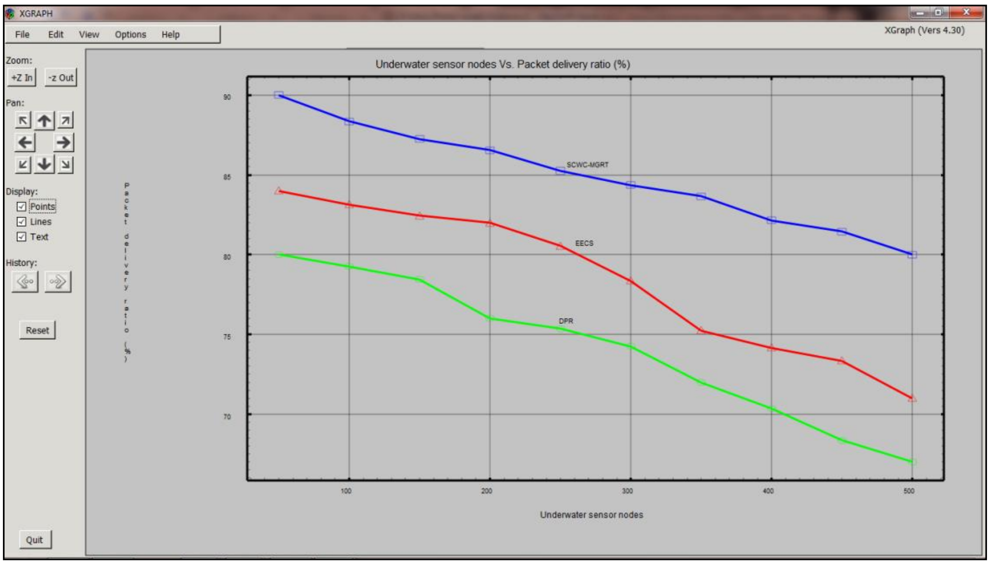

Figure 5. Graphical Representation of Packet Delivery Ratio

The packet delivery ratio is established in Figure 5. First-stage trust evaluations, i.e., distance trust and mobility trust, are measured, following which, in the second stage, secure routing is ensured via the Memory Centered Gated Recurrent model. Only upon successful validation of results stored in the Memory Centered Gated Recurrent Unit is secured routing ensured between the underwater sensor nodes, following which packet delivery is made. The packet delivery ratio using the SCWC-MGRT method was enhanced by 8% compared to [1] and 15% compared to [2], respectively.

6. Conclusion

In this paper, we proposed energy-efficient SCWC-MGRT secured routing in UWSN. The method provides energy-saving and reliable data transmission by combining the advantages of the Steiner Chinese Whisper Node Clustering algorithm and Memory-Centered Gated Recurrent Trust-based secure routing. In SCWC-MGRT, we identify the Steiner Triangulation point for each node and measure the energy consumed to forward data packet design. Following this, the identification of groups of underwater sensor nodes that broadcast the same data packet to their adjacent nodes is measured, and clusters are formed accordingly. The data packet forwarding to adjacent nodes based on similar data packets can contribute to disabling unused nodes during the cluster head selection process, meanwhile minimizing the energy consumption and end-to-end delay. Furthermore, we designed a secured routing model by obtaining trust via the relationship between underwater sensor nodes using the fitness function and applied it to a centred Gated Recurrent Unit for validating the routes. The outcome of SCWC-MGRT has the best performance by different factors. In limitations or challenges proposed by the SCWC-MGRT approach, nodes are resource-constrained in terms of energy, computational capability, storage capacity, and communication range. Sensor nodes in UWSN are resource-constrained devices that have restricted energy, memory size, and communication ability as well.

References

[1] H. H. Rizvi, S. A. Khan, R. N. Enam, M. Naseem, K. Nisar, and D. B. Rawat, “Adaptive energy efficient circular spinning protocol for dynamic cluster based UWSNs,” *IEEE Access*, vol. 10, pp. 61937-61950, 2022.

[2] A. Alharbi, A. M. Abbas, and S. Ibrahim, “Securing localization-free underwater routing protocols against depth-spoofing attacks,” *Array*, vol. 13, p. 100117, 2022.

[3] O. Gupta, N. Goyal, D. Anand, S. Kadry, Y. Nam, and A. Singh, “Underwater networked wireless sensor data collection for computational intelligence techniques: issues, challenges, and approaches,” *Ieee Access*, vol. 8, pp. 122959-122974, 2020.

[4] R. T. Rodoshi, Y. Song, and W. Choi, “Reinforcement learning-based routing protocol for underwater wireless sensor networks: a comparative survey,” *IEEE Access*, vol. 9, pp. 154578-154599, 2021.

[5] S. Khisa, and S. Moh, “Survey on recent advancements in energy-efficient routing protocols for underwater wireless sensor networks,” *IEEE Access*, vol. 9, pp. 55045-55062, 2021.

[6] X. Wei, H. Guo, X. Wang, X. Wang, and M. Qiu, “Reliable data collection techniques in underwater wireless sensor networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 404-431, 2021.

[7] S. Bharany, S. Sharma, N. Alsharabi, E. Tag Eldin, and N. A. Ghamry, “Energy-efficient clustering protocol for underwater wireless sensor networks using optimized glowworm swarm optimization,” *Frontiers in Marine Science*, vol. 10, p. 1117787, 2023.

[8] Y. Hu, K. Hu, H. Liu, and X. Wan, “An energy-balanced head nodes selection scheme for underwater mobile sensor networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 63, 2022.

[9] A.V. Bharathy, and K. K. C. Rao, “One-leap fuzzy enabled clustering technique for under water wireless sensor networks to improve the stability and energy exhaustion rate of the nodes,” in *Journal of Physics: Conference Series*, vol. 1172, no. 1, IOP Publishing, Mar. 2019, p. 012080.

[10]Q. Bai, and C. Jin, “A K-means and ant colony optimization-based routing in underwater sensor networks,” *Mobile Information Systems*, vol. 2022, pp. 1-12, Apr. 2022, doi: https://doi.org/10.1155/2022/4465339.

[11]K. Lavanya, K.V. Devi, and B.R. Bapu, “Deep Reinforcement Extreme Learning Machines for Secured Routing in Internet of Things (IoT) Applications,” *Intelligent Automation & Soft Computing*, vol. 34, no. 2, 2022.

[12]A. Venkatesh, and S. Asha, “DERNNet: Dual Encoding Recurrent Neural Network Based Secure Optimal Routing in WSN,” *Computer Systems Science & Engineering*, vol. 45, no. 2, pp. 1375-1392, 2023.

[13]N. Hemavathy, and P. Indumathi, “Deep learning-based hybrid dynamic biased track (DL-HDBT) routing for under water acoustic sensor networks,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1211-1225, 2021.

[14]R. Huang, L. Ma, G. Zhai, J. He, X. Chu, and H. Yan, “Resilient routing mechanism for wireless sensor networks with deep learning link reliability prediction,” *IEEE Access*, vol. 8, pp. 64857-64872, 2020.

[15]Y. Su, R. Fan, X. Fu, and Z. Jin, “DQELR: An adaptive deep Q-network-based energy-and latency-aware routing protocol design for underwater acoustic sensor networks,” *IEEE Access*, vol. 7, pp. 9091-9104, 2019.

[16]H. Tran-Dang, and D. S. Kim, “Channel-aware energy-efficient two-hop cooperative routing protocol for underwater acoustic sensor networks,” *IEEE Access*, vol. 7, pp. 63181-63194, 2019.

[17]A. Alharbi, “DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 9, 2020.

[18]K. Saeed, W. Khalil, S. Ahmed, I. Ahmad, and M. N. K. Khattak, “SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks,” *IEEE Access*, vol. 8, pp. 107419-107433, 2020.

[19]T. Dargahi, H. H. Javadi, and H. Shafiei, “Securing underwater sensor networks against routing attacks,” *Wireless Personal Communications*, vol. 96, pp. 2585-2602, 2017.

[20]R. Muthukkumar, and D. Manimegalai, “Secured transmission using trust strategy-based dynamic Bayesian game in underwater acoustic sensor networks,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 2585-2600, 2021.