



Joint trust-based detection and signature-based authentication technique for secure localization in underwater wireless sensor network

Manni Kumar¹ · Nitin Goyal² · Ramy Mohammed Aiesh Qaisi³ · Mohd Najim³ · Sachin Kumar Gupta⁴

Received: 23 November 2023 / Revised: 11 October 2024 / Accepted: 4 February 2025

Published online: 17 February 2025

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2025

Abstract

Ensuring secure and accurate node localization in Underwater Wireless Sensor Networks (UWSN) is a significant challenge, as conventional methods tend to neglect the security risks associated with malicious node interference. This research addresses this issue by proposing a Joint Trust-based Detection and Signature-based Authentication (JTDSA) technique, aimed at improving both the security and accuracy of node localization in UWSNs. The technique utilizes Intrusion Detection System (IDS) methods to calculate the trust values of secondary-anchor nodes (SNs), ensuring only the most trusted SNs are selected. Furthermore, a digital signature algorithm secures the Received Signal Strength (RSS) data from tampering. The method incorporates a hybrid approach combining Angle of Arrival (AoA) and RSS ranging techniques to achieve robust localization. Simulation results demonstrate that JTDSA improves localization accuracy by 4% compared to existing methods, achieving an overall accuracy of 99.2%. The technique also reduces packet drop by 35% and enhances attack detection accuracy by 3%. These results indicate that the proposed JTDSA technique offers an effective solution for secure and reliable localization in UWSNs.

Keywords AOA · Game Theory · Hybrid Localization · Received Signal's Strength (RSS) · Underwater Wireless Sensor Network (UWSN)

1 Introduction

Underwater wireless sensor networks (UWSNs) have recently received increasing attention owing to their wide applicability in areas such as ocean resource exploitation and monitoring, tracking of ocean-going vessels, and disaster prevention. Accuracy and reliability are critical in these applications. Several network system operations are executed, such as managing network topology and developing protocols related to communication. Thus, the sensor nodes should be localized [1]. Reference nodes and non-localized nodes are the two main kinds of nodes in the UWSN deployment. These are the anchor nodes and

the localized nodes. Non-localized nodes, on the other hand, are those nodes whose exact position is unclear. The anchor nodes often get their locations from GPS or surface buoys, accordingly. However, existing localization approaches in UWSNs pose substantial security risks. Traditional approaches, such as Received Signal Strength (RSS)-based localization, Angle of Arrival (AoA), and hybrid models, frequently fail to address security issues successfully. Malicious nodes can modify beacon messages, resulting in faulty localization and even network intrusions. While other solutions use intrusion detection systems (IDS) or trust-based models, they either fail to identify all types of malicious assaults or have a large processing burden, making them unsuitable for real-time underwater applications [2]. Non-localized nodes are first brought into proximity to the anchor nodes, which serve as the starting point for the localization process. It is possible for non-localized nodes that have been successfully localized to serve as references for the rest of the non-localized nodes [3].

Energy consumption, battery consumption, cost, power, deployment of nodes, routing, bandwidth, and storage capacity are some of the challenges of such networks [4]. The WSN's random deployment and changing network topology make it susceptible to a range of hazards. Secure localization methods are extensively utilized for secure data transmission [5]. With no real-time communication and limited resources, installing a UWSN in such a hostile environment creates a variety of security and performance problems. Sensors are forced to store a huge quantity of data, including their authentication information because they cannot offload the sensed data. Unattended settings, on the other hand, leave the UWSN open to active and/or mobile hackers. In the event of a physical attack, an adversary might seize control of sensors and obtain access to collected data and cryptographic keys. After an assault, an adversary with access to a sensor's cryptographic keys may use those keys to produce fake messages. However, it is essential to ensure that the sender's data is not changed by the adversary before the opponent takes control. Forward security refers to this kind of security [6–8].

Two main security requirements that get achieved using forward secure and aggregate signatures are Data integrity and authentication in the presence of active adversaries. UWSNs cannot handle computational, memory, and communication overheads associated with existing forward security and aggregate signature techniques. So, it becomes very difficult and thus imperative to find more flexible and efficient forward-security-aware and aggregate signatures for UWSNs [9–11]. Numerous localization schemes have been proposed for node tracking and locating but very little work has been done for node security while positioning information extraction. There may be a chance that an outside node may enter our network and begin to steal information as a part of the network [12].

Existing localization methods in UWSNs inadequately address security vulnerabilities, making them susceptible to attacks such as data modification, selective forwarding, and denial of service (DoS). These limitations hinder the reliability of localization, leading to potential network breaches and compromised operational integrity. To solve the stated security problems, we propose a novel Joint Trust-based Detection and Signature-based Authentication (JTDSA) approach. This method uses an IDS framework to calculate the trust levels of SNs, assuring that only the most trustworthy nodes participate in the localization process.

This research's main aims to deal with this security issue of node localization and provide secure communication in the network. In this technique, among the number of Secondary-anchor Nodes (SNs), one Primary-anchor Node (PN) is equipped with a strong signal processor while other SNs are equipped with simple single-antenna transceivers. In this hybridization, AoA is estimated from the PN only while the RSS is measured from

the selected set of SNs. Only a few of the numerous suggested locating algorithms for UWSNs addressed reliability or security concerns. Anchor and reference sensor nodes may be authenticated using trust models or identified using IDS methods in current localization security research. Beacon messages sent by trustworthy anchor nodes might, however, be tampered with by malicious intermediary nodes. Unknown nodes also have the power to reshape the position data of legitimate reference nodes in a similar manner. Furthermore, to avoid manipulation, RSS measurements are digitally signed, which ensures the integrity of data exchanged between nodes. Hence, the main contributions of our work are as follows:

- i. Proposed a novel approach, JTDSA technique that integrates trust evaluation with digital signature mechanisms for secure localization in UWSNs.
- ii. Utilizing an IDS framework to compute trust values for SNs, effectively mitigating risks from malicious nodes and ensuring the integrity of localization data.
- iii. Hybrid localization that Combines AoA and RSS measurements to improve localization accuracy while safeguarding against data tampering.
- iv. Compare the performance with existing methods to signify the effectiveness of the proposed technique in real-world scenarios.

Further, the rest work of this article is organized as follows: Section 2 provides a comprehensive review of related work of existing studies and finds out the research gap. Section 3 details the proposed secure localization technique including methodology and algorithms employed. Section 4 presents the stimulation parameter settings to analyze the performance. Finally, the conclusion and future work is described in Sect. 5.

2 Literature survey

Numerous researches have already been done to provide security in Wireless Sensor Network (WSN) but only a few researches have been done yet in the network field of UWSNs. Since of the various characteristics of the aquatic or ocean environment such as communication medium (i.e., acoustic medium), limited battery, node mobility, temperature, etc. Rather than these challenges and issues, several localization schemes proposed in UWSN provide security and privacy to nodes while communicating [13, 14]. In this section, some of the recent proposed methods are discussed.

Despite the advancements developed, substantial research gaps remain, notably in the integration of strong security procedures with localization techniques. For example, the paper entitled [15] “A Dataset for Recognition of Norwegian Sign Language” underlines the significance of correct data representation in communication systems, illustrating how exact localization data is critical for UWSN. However, this study focuses exclusively on human–computer interaction and does not address the security issues required for accurate localization in sensor networks. As a result, the lack of safe data processing procedures creates a substantial gap in the integrity of localization information [16].

Collaborative Secure Localization (CSLT) for UWSNs has been suggested by Han et al. [17]. According to this mechanism, it calculates trust values based on the Trust Model. The trust evaluation of anchor nodes, the first position of unknown nodes, the selection of a reference node, and the secondary placement of an unknown node are all stages of this method. The proposed CSLT approach is better than prior compared techniques on the basis of some parameters such as security provided due to location, accuracy achieved, and

calculating ratio based on localization. Although various types of malicious attacks were detected, some types could not be efficiently identified.

Shanthi et al. [2] designed a probabilistic model-based framework for safe localization. When tested empirically, this new localization framework exceeds the current one in terms of security effectiveness. But, due to the fixed computational load, there is an increase in the execution time. For short-distance 2D UASN, Shukla et al. [4] have presented an event-driven distributed localization technique. Using recursive localization, the proposed design leverages an efficient node as a reference node to assist in the localization of additional sensor nodes. Using a recursive localization approach, the suggested system may achieve better power consumption, packet delivery ratio, and delay reduction. NS2.35 is used for the simulation.

Using PSO and Gradient Descent Methods, Shanthi et al. [18] have developed a secure location for underwater wireless sensor networks (UWSN). At this step, malicious nodes may be excluded from participating in the localization process by combining GD with machine learning (ML). The best outcome is given by PSO in today's global space using the set of non-malicious nodes that were previously selected. In the presence of malicious nodes, the combined strategy of Particle Swarm Optimization (PSO) and Graph Density (GD) yields better outcomes than the two approaches applied independently, according to the experiments. However, the scalability of the localization can be increased.

Hu et al. [19] proposed a CTLAS strategy that can be applied to VaNET. the CTLS and AGSS scheme is revived and then the security of this scheme is analyzed by a detailed attack process. The improvement of the existing scheme is provided with an efficient method. The problem with this method is that if the malicious node obtains a temporary key, then a malicious node can forge a signature for any node.

Yan et al. [20] identified the node location's privacy issue and proposed a solution for safe node localization. It is named as Deep Reinforcement Learning (DRL) method and for providing security is considered the UWSNs scenario of supervising, unsupervised, and semi-supervised environment of sensor nodes where a ray-compensation technique is used to overcome the localization error. Although it provides privacy and accuracy it has the scope of improvement that it does not consider the mobility of nodes.

Elhoseny et al. [21] proposed a unique content-efficient decision-aware task scheduling (CATSA) strategy to improve the performance of sensor-aware distributed workflow applications in underwater environments. Recognizing the increasing complexity of maritime activities that create and analyze data, the authors emphasize the issues given by network content, workload changes, execution durations, deadlines, and bandwidth limits. The paper tackles the requirement for effective scheduling methods in mobile workflow systems, which can be challenging owing to the shifting factors. CATSA efficiently adapts to complex environmental changes by integrating several components such as a decision planner, sequencing, and scheduling routines. After thorough testing, the architecture outperformed prior solutions by 30% in workflow execution quality and 40% in timeline adherence. However, the study's relevance is potentially restricted because it is based on specific environmental circumstances that may not be indicative of other underwater environments.

Misra et al. [22] have proposed SecRET, which is treated as a very secure localization approach. Moreover, this approach is supported by some theory based on evidence for UWSNs; in which a non-localized node may pick the most trusted collection of anchors with minimal resource usage using SecRET, a trust-based computation technique. As a result, the suggested strategy can adapt to a wide range of threats in the UWSN setting. Even with compromised nodes under various attacks, the performance assessment based on NS-3 shows that SecRET maintains the deployed nodes' energy efficiency while

maintaining efficient and secure localization. However, only some of the known attacks have been taken into consideration.

Dong et al. [4] propose a secure and precise localization approach for mobile nodes in underwater acoustic sensor networks, which addresses issues such as malicious nodes, mobility, and fluctuating sound speed. The technique enhances localization accuracy by combining an anchor node screening mechanism, an Unscented Kalman filter, and real-time sound velocity profiles, as demonstrated by simulations and reservoir tests. The intricacy of real-time sound velocity measurements, as well as the computing overhead, may limit its usefulness. Future research might focus on enhancing these characteristics for greater scalability and efficiency in more substantial more dynamic underwater conditions.

Furthermore, Table 1 provides the analysis of secure localization schemes for better understanding.

On the basis of the above carried out analysis, it has been found that a secure node localization technique is still required to protect the network from the leakage of the node's position information. While providing secure node communication it is also necessary to maintain the accuracy and residual energy of nodes along with minimum packet loss. The next section elaborates on the technical details to solve this problem.

3 Proposed methodology

Most localization schemes neglect node security. We proposed a technique that assures the authentication of the node for communication in the network and protects it from information leakage. For this purpose, a joint trust model with digital signature identification is used and for node position estimation hybrid RSS and AoA ranging techniques are used.

4 System model

In this technique, UWSN the N anchor nodes whose position is known is taken into consideration. Among the N anchors, there is one PN node that gets embedded with the high-energy antenna in the form of an array-like structure followed by high signal processing conditions, while other SNs are equipped with simple single-antenna transceivers. To reduce the computational overhead of AoA, this AoA is estimated from the PN only while the RSS is measured from the selected SNs.

So, the nodes that are following particular communication systems in UWSNs; get attacked very easily by false data unintentionally from nearby neighboring nodes resulting in a depletion of energy. The following attacks are considered in this work: Denial of Service (DoS), selective forwarding, good/bad-mouthing, and data modification attacks.

5 Overview

We propose a joint trust-based detection and signature-based authentication technique for secure node localization in UWSNs. There are four phases of our methodology:

In 1st phase (Trust-Based Node Selection): IDS is used to evaluate the trustworthiness of secondary-anchor nodes (SNs) based on interaction efficiency and response delay.

Table 1 Comparison of existing secure localization schemes in UWSNs

Ref	Proposed Scheme	Summary	Advantages	Drawbacks
Han et al. [17]	CSLT	Tryst mechanism is implemented and localization is divided into four stages i.e., calculating the trust value of nodes, followed by finding a position of nodes that are not known; then evaluating the trust of referred nodes; choosing the referred node, and then localizing the unknown nodes	It helps in enhancing the security of positioned nodes. Helps in increasing the accuracy of position and also improves the localization ratio	This method can find only some of the attacks and couldn't manage all attacks efficiently
Misra et al. [22]	SecRET	This technique is based on Evidence theory using SecRET, a non-localized node selects the most trustworthy set of anchors while consuming the fewest resources	Provides secure localization and energy efficiency	Considers only some known attacks
Shanthi et al. [2]	SLPA	A probabilistic model-based safe localization framework is described	Enhance the security of nodes	Execution time increases due to fixed computational load
Hu et al. [19]	AGSS	This method revives AGSS and presents a security analysis for it	Analyze the security of CTSLS and provide a security improvement	If the temporary key is known to the user, then the user can forge a signature
Shanthi et al. [18]	SL	Secure localization is done using PSO and GD	Less energy consumption and better localization ratio	The scalability of localization can be increased
Yan et al. [20]	DRL	Supervised, unsupervised, and semi-supervised sensor nodes are considered for localization using deep learning	Overcome the localization error rate and provide security to nodes,	Energy consumption and node mobility have not been considered for localization
Dong et al. [4]	SALM	Utilizing an anchor node screening mechanism, Kalman filter, and sound velocity, to improve localization accuracy	Enhances accuracy by mitigating errors from malicious nodes, mobility, and variable sound speed	Computational overhead required for accurate localization

Malicious nodes are identified and isolated, while the most trustworthy nodes are selected for the localization process.

In 2nd phase (Digital Signature Authentication): After node selection, the RSS measurements from these trusted SNs are digitally signed. This ensures that the data remains unaltered during transmission and protects against external attacks.

In 3rd phase (Hybrid Localization—AoA + RSS): It combines AoA measurements at primary-anchor nodes and RSS from trusted SNs, enhancing localization accuracy by utilizing the strengths of both techniques.

In 4th phase (Performance Evaluation): The method is evaluated through simulations to demonstrate the robustness of the approach by showing improvement in localization accuracy, less packet drops, and attack detection.

The block diagram of the proposed JTDSA technique is depicted in Fig. 1. That shows, when the unknown sensor node sends a localization request (Loc_{req}) to SA, the SA sends a localization reply (Loc_{rep}). Then, the sensor node calculates the direct trust value for the SA using the metrics of interaction efficiency and response delay. The total trust values of the SNs are estimated from the direct and indirect trust values so that the SNs with maximum trust values are selected. The RSS measurements from the selected SNs are digitally signed and transmitted to the sensor nodes, where the sensor nodes verify the signatures to retrieve the RSS values.

6 Estimation of RSS and AoA

As discussed in brief, there are some issues and errors in calculating the exact position of nodes. Also, the concept of RSS localization could not accurately predict the node's deployment position. Therefore, if a combination of AOA estimation is used with the concept of

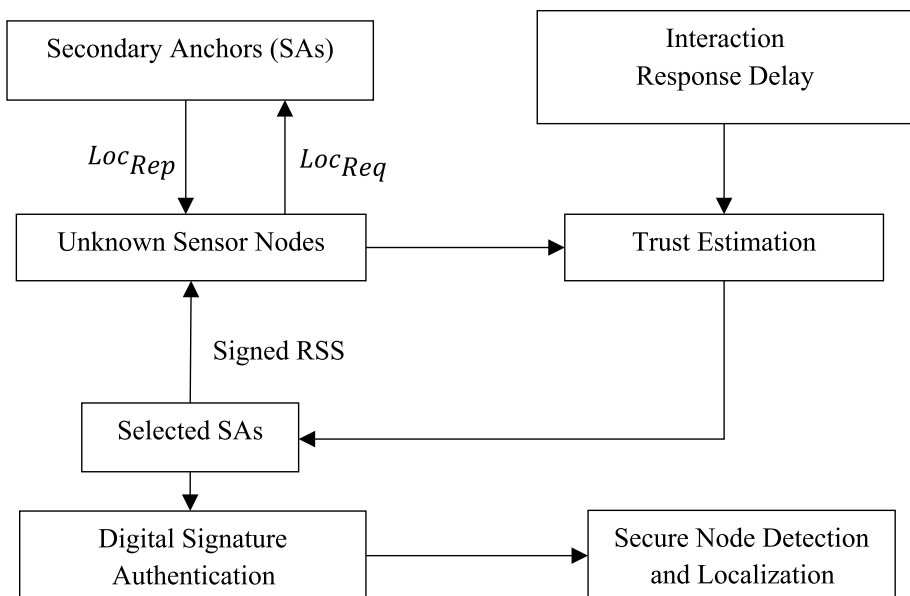


Fig. 1 Block diagram of JTDSA technique

range, then the chances of increase in accuracy become very high. Assume a UWSN that consists of N anchor nodes whose position is given by $[a_i = a_{ix}, a_{iy}], i = 1, \dots, n$ and M node whose actual locations are $[x_n = x_{mx}, x_{my}], i = 1, \dots, m$. At the anchor (a_i), the RSS (rs_i) and AOA (α_i) measured from the m_{th} node is expressed as

$$rs_i = rs_0 - 10\gamma \log_{10} \left(\frac{\|x_m - a_i\|}{r_0} \right) + n_i \quad (1)$$

$$o_i = \tan^{-1} \left(\frac{x_{my} - a_{iy}}{x_{mx} - a_{ix}} \right) + m_i \text{ for } i = 1, \dots, n \quad (2)$$

where, rs_0 depicts the power received at a particular reference distance denoted as r_0 , γ exhibits the exponent related to the loss of path, $\| \cdot \|$ depicts the Euclidean norm, n_i is the log-normal shadowing, and m_i depicts noise due to estimating the angle of location. These n_i and m_i are treated as Gaussian random variables possessing zero-mean with standard deviations $\sigma_{n_i}(db)$ and $\sigma_{m_i}(degree)$, respectively i.e., $n_i = n(0, \sigma_{n_i}^2)$, $m_i = n(0, \sigma_{m_i}^2)$. Also, the main problem lies in estimating proper location of the agent x_m based on p_i and a_i . Equation (1) which might get solved through estimating the distance D using graph technique. An approximation on using the concept of corresponding distance is solved numerically between the anchor node and the normal sensor. As shown in Fig. 2, an anchor node (red star) comes inside the selected optimum set of SNs and all SNs are selected by the PA only for the localization process. PA computes the position of the node using the AoA ranging

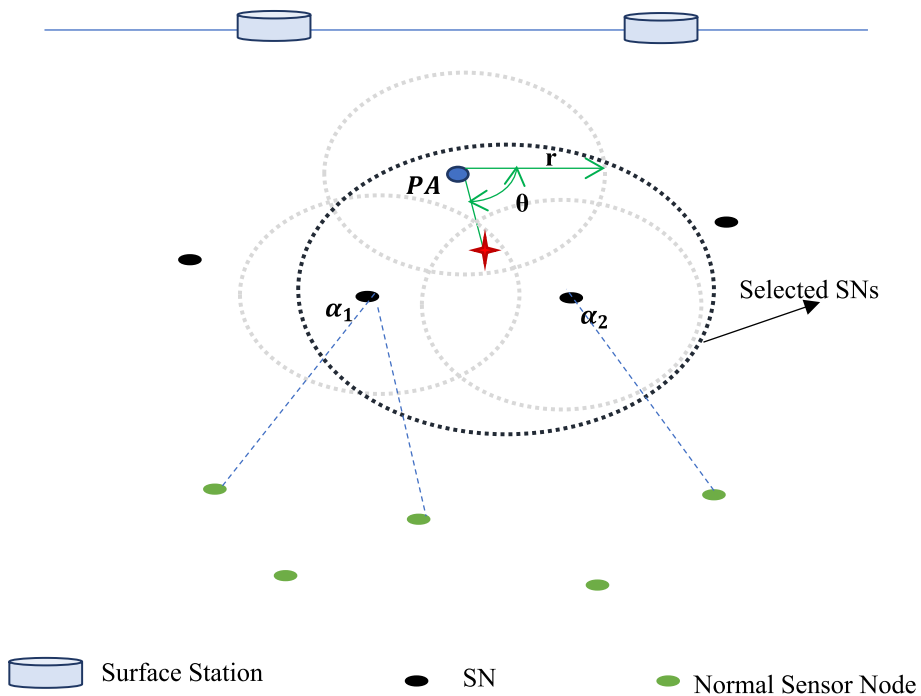


Fig. 2 Hybrid localization in UWSN

method and the authenticity is evaluated on the base of the trust model. After the surety of authenticity of the node then further that node is used for the localization of the normal sensor using RSS measurement.

6.1 Trust evaluation metrics

In the UWSN technique which is based on localizing the points, the sensor node that is unknown i.e., N sends the localization request (*LocReq*), and the other node α ; that lies in the transmitting range of UN , sends the reply to node N ; whenever the request is received. Then, N calculates DT also called as direct trust value for node α using the following two metrics:

6.1.1 Interaction efficiency (*IE*)

It is derived based on the successful and failed interactions with an anchor node by a sensor node.

$$IE = No_Success / Tot_trans \quad (3)$$

where, $No_success$ denotes the number of successful transactions and Tot_trans denotes the total number of transactions.

6.1.2 Response delay (*RD*)

It is the time taken between issuing the *LocReq* to the anchor node and obtaining *LocRep* to the requested service.

$$RD = TLoc_{Rep} - TLoc_{Req} \quad (4)$$

where, $TLoc_{Rep}$ and $TLoc_{Req}$ are the time of issuing *LocReq* and time of receiving *LocRep*, respectively. Then DT is computed by

$$DT = \alpha.IE + \beta.RD \quad (5)$$

where α and β represent weighted coefficients of the metrics.

All previous DT values are combined in order to obtain the final result:

$$D_{xy} = \prod_{k=1}^n DT_k \quad (6)$$

where, DT_k indicates the K^{th} value of DT , D_{xy} indicates the direct trust value of the source node x for target node y .

6.1.3 Indirect trust and recommended trust

The proposed model consist of three kind of sensor nodes known as the one which is sending the data i.e., source node (S), second is the node to which data has to be sent i.e., the target node (T), and the recommended node (R). Other beacon nodes, which are within the communication range of node N , form the recommended node set defined as $R = \{B_1, B_2, \dots B_i\}$.

In order to get indirect trust value (IT) of node B , node N calculates the recommended trust value of nodes in R . Hence the cumulative trust value (CT) is defined as

$$CT_{xy} = DT_{xy} + IT_{xy} \quad (7)$$

The trust-based SA selection is illustrated in the following algorithm:

Algorithm 1 Trust-based SA node selection

Input: Set of SNs(SA_j), ($j = 1, 2 \dots N$)

Set of unknown sensor nodes N_i , $i = 1, 2 \dots M$

DT_{ij} , Direct trust of source N_i for target SA_j .

Output: Set of trusted SAs $\{OptSA\}$

1. $\{OptSA = \emptyset\}$
 2. **while**($t < T$)
 3. **for each** SA_j ,
 4. N_i estimates IE and RD
 5. N_i computes DT_{ij} using Eq. (6)
 6. N_i computes IT from recommended trust values
 7. N_i computes cumulative trust CT_{ij} using Eq. (7)
 8. **if**($CT_{ij} > trust_{min}$)
 9. Add SA_j into $\{OptSA\}$
 10. **end if**
 11. **end for**
 12. $t = t + 1$
 13. **end while**
-

In this algorithm, the SNs with cumulative trust values higher than a minimum trust threshold ($Trust_{min}$) are selected as optimum SNs.

6.2 Signature-based authentication

In this section, the RSS values from the N SNs are digitally signed and verified at the sensor node end. Signature-based authentication is intended to provide public verifiability, high efficiency, and forward security. There are certain items of data which needs to be encrypted by the concept of chaining roots, followed by decryption which in return needs to be verified by the receivers by releasing the time of trapdoor keys.

Also, the key at initial level called as per-interval is generated by Trusted Server (TS) generates i.e., Z_0^i for particular sender i . This key gets updated when the time gap gets vanished and also when there is start of new time gap. To derive the chain root, $k_0^{i,W}$ in every interval of time interval T_w , then also the concept of this key is used. Along with, it will be used to calculate the aggregate signatures in T_w . The TS encrypts each $k_0^{i,W}$ with tk_w^i so that encrypted value of chain root C_i^W is obtained. The detailed explanation is given below:

6.2.1 Initialization phase

- 1) The synchronization error calculated by TS is depicted as $8t$ and there is release of trapdoor depicted as $0 < T_0 < T_1 < \dots < T_{L-1}$ depending on need of requirement of

applications. There exist two consecutive time levels depicted as T_{i-1} and T form the i_{th} time interval T_i .

- 2) This hash chain which is also used in initialization is also generated by $TSV_w = H_1(v_w - l)$ for $w = 1, \dots, L - 1$, in which all the elements are used as the secret trapdoor keys in the reversed form depicted as $tk_w = V_{L-l-w}$ for $w = 0, \dots, l - 1$. So, value of each tK is linked with the above discussed time interval for $w = 0, \dots, l - 1$. The encrypted chain roots depicted for every sender i is depicted below:
 - a) The n -bit per-interval key Z_l^0 is generated for every sender i . Concept of chain root for every interval discussed above T_w is exhibited as $K_0^{i,w} = H_2(Z_w^i)$ and $Z_{w+1}^i = H_1(Z_w^i)$ for $w = 0, \dots, L - 1$
 - b) The session keys in the entire network are generated as $tK_w^i = H_3(tK_w || ID_i)$; followed by chain root which is encrypted of sender i for time period t was $C_w^i = E_{tki}(K_0^{i,w})$ where $w = 0, \dots, l - 1$.
- 3) The maximum synchronization error is given by TTP and is transmitted to all receivers, followed by interval key, then the chain roots which are in encrypted form and clock error $ID_i, Z_0^i, C_0^i, C_1^i, \dots, C_{L-1}^i, \partial t$ to each sender i . There is a phase called as Trapdoor Release Phase which is executed in two modes:
 - i. **Synchronous Mode:** This is determined according to pre-determined time schedule, at the end of each tw , after this process there is release of trapdoor key by TTP, tk_w .
 - ii. **Asynchronous Mode:** For releasing secret key receiver sends the request message to TTP; so that the time trapdoor key is released when she is ready for data transmission. So, secret key is released when TTP receives requests more than particular threshold value i.e. (authenticated) requests (e.g., $t = 90\%$).

6.2.2 Signature generation at the SNs

- 1) When the time interval starts i.e., t_w , SA_i the item key is derived as $K_0^{i,w} = H_2(Z_w^i)$, followed by updation key as $Z_{w+1}^i = H_1(Z_w^i)$; followed by deletion of Z_w^i from memory.
- 2) SA_i has accumulated data items $D_0, D_1, \dots, D_{Z-1}$ followed by computation of aggregation signature $\sigma_0^{i,w}$ in t_w . When SA_i collects D_i , it first computes the individual signature of D_i as at $\sigma_0^{i,w} = \text{MACK}_t^{i,w}(D_i)$, where $Z_{w+1}^i = H_1(Z_w^i)$, and then folds a; 'w into $tK_w^i = H_3(tk_w || ID_i)$.

6.2.3 Signature verification at the sensor nodes

- 1) Assume that a sensor node N_k has received $ID_i, D_0^i, D_1^i, D, \dots, D_{L-1}^i$, at time t . In the synchronous mode, N_k checks whether the timing condition $(t + \delta t) \leq tw$ holds for $\sigma_0^{i,w}$. If yes, N_k tries to buffer the gathered signatures along with the data set and also waiting for the end of t_w to obtain tk from the TTP.
- 2) In the asynchronous mode, to obtain tk_w , the N_k sends a request to the TS .
- 3) When the TS releases tk_w each N_k verifies tk_w by checking whether $tk_w = H_1(tk_{w-1})$. If tk_w is verified, then N_k verifies $\sigma_0^{i,w}$ as follows:

- 4) N_k decrypts $c \sim$ by computing $tK_w^i = H_3(tk_w || ID_i)$ and $\sigma_0^{i,w}$. By using the same key per- data item N_k computes individual signatures of $\sigma_0^{i,w} = \text{MACK}_t^{i,w}(D_l)$. and updates $K_{j+1}^{i,w} = H_1(k_j^{i,w})$ for $1 = 0 \dots 1$.
- 5) Finally, N_k computes $k_{0,j}^{i,w} = H_3(\sigma_{0,j-1}^{i,w} || \sigma_{0,j}^{i,w})$ where $\sigma_{0,0}^{i,w} = \sigma_0^{i,w}$, and $\sigma_{0,0}^{i,w} = \sigma_0^{i,w}$ checks. If they match, N_k accepts $\sigma_{0,l}^{i,w}$; otherwise, reject.

7 Evaluation and analysis

The particular section measures performance parameters to evaluate the proposed work on simulator using some QoS matrices.

7.1 Simulation parameters

This method is validated for secure localization concept in UWSN. Along with this, it uses AquaSim toolkit for evaluating the results. This AquaSim simulator finds the attenuation of the acoustic signal and packet collisions for all the data that is sent from source to receiver. An object-oriented design is followed along with support of three-dimensional structure. For simulation, the UWSN area was $1000 \text{ m} \times 1000 \text{ m} \times 100 \text{ m}$, and the node transmission range was 200 m. Further, the simulation settings and parameters for underwater network communication are summarized in Table 2.

Table 2 Simulation set-up

Parameters	Values
Number of Nodes	25,50,100,125 and 150
Area size	1000X1000x100m3
MAC Protocol	Underwater Mac
Simulation Time	100 s
Channel	Underwater Channel
Range	200 m
Routing Protocol	Vector based Forward
Antenna Type	Omni Antenna
Initial Energy	10,000 Joules
Transmission power	2.0 watts
Receiving Power	0.75 watts
Idle Power	0.008 watts
Frequency	25 kHz
Packet Size	25 bytes
Interval	100
Position Update Interval	0.3
Minimum and a maximum speed of nodes	0 to 3 m/s

7.2 Simulation results

The proposed JTDSA technique is compared with SecRET [22], SALM [4], and Secure Localization Model Based on Trust Valuation SL [2] approaches according to the metrics localization latency, localization accuracy, attack detection accuracy, average residual energy, and packet drop.

7.2.1 Packet drops (Pk_D)

It is computed as the number of packet loss over the total transmitted packets to the receiver. It is formulated as:

$$Pk_D = Totalpackets - Recievedpackets \quad (8)$$

From Fig. 3, it can observe that as the number of nodes is increased, the packet drop increases linearly, due to the chances of more attacks. Whenever DoS or selective forwarding attack occurs, it results in more failed transactions and delayed response. Hence the proposed JTDSA reduces the packet drop due to these attacks, from the trust metrics of interaction efficiency and response delay. The result shows the JTDSA achieves 35% lesser latency than SL, 10% lesser latency than SALM, and 18% lesser than SecRET for different nodes scenarios since JTDSA reduces the packet drop due to DoS and selective forwarding attacks employing trust metrics. The reduction in packet loss rates is mostly attributable to the digital signature verification procedure, which assures the data's integrity while being transferred. JTDSA ensures a trustworthy communication channel by effectively identifying and isolating rogue nodes, improving the network's overall performance.

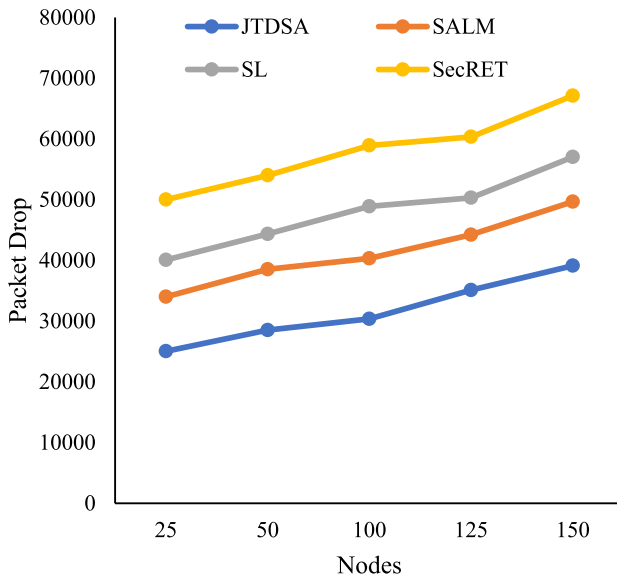


Fig. 3 Packet drop for nodes

7.2.2 Residual energy

It is measured as the total energy of the node minus the used amount of energy. It is expressed as:

$$Res_E = T.E - U.E \quad (9)$$

where

Res_E Residual energy
 $T.E$ Total energy of node
 $U.E$ Energy used by node

The localization process consumes energy for estimating the position of the node. Therefore, the involvement of more nodes in the localization system leads to higher energy consumption. The JTDSA technique is designed to minimize energy overhead by selectively activating only the most trusted SNs for localization, thereby reducing unnecessary energy expenditure on compromised or unreliable nodes. Additionally, the lightweight digital signature algorithms used in JTDSA further conserve energy during data transmission and processing.

From Fig. 4, it can be observed that the JTDSA achieves 36% higher residual energy than SL, 24% higher than SecRET, and 15% higher than SALM in various node scenarios. This improvement in residual energy is attributed to JTDSA's ability to mitigate flooding attacks and its strategic use of a limited set of SNs, which enhances overall energy efficiency in the network.

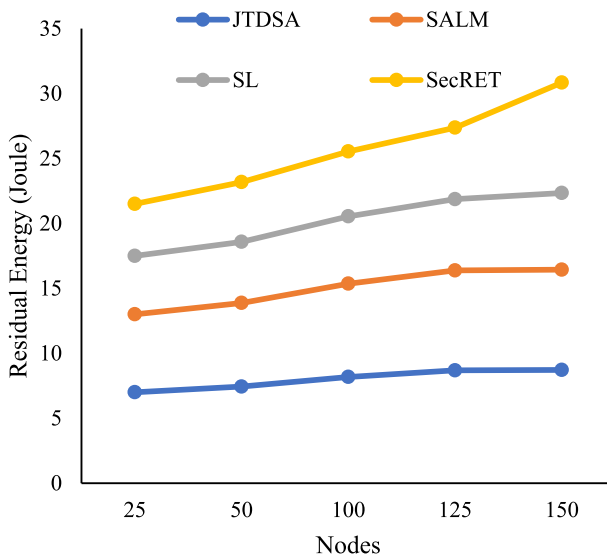


Fig. 4 Residual energy for nodes

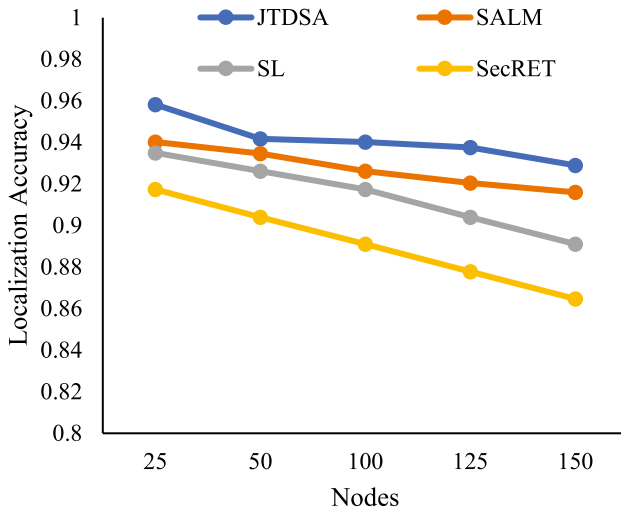


Fig. 5 Localization accuracy for nodes

7.2.3 Accuracy

It is defined as the percentage of accurate estimation of the node's position. It can be computed as the ratio of estimated position by the actual position of the node. It is directly depending upon the error rate such as if the error rate decreases accuracy increases.

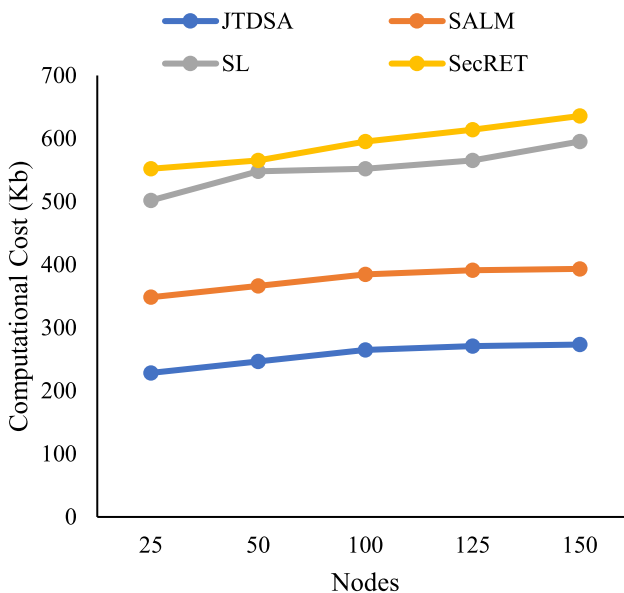


Fig. 6 Computational cost for nodes

Figure 5 shows the accuracy of various localization methods for UWSNs. When nodes are added during localization, the error increases owing to the increased rate of packet collisions. Furthermore, the proposed JTDSA achieves 4% higher localization accuracy than SL, 2% higher than SALM, and 3% higher than SecRET for different node scenarios, due to the hybrid AoA/RSSI-based localization technique of JTDSA. This improvement is due to the use of trust-based node selection and hybrid localization techniques (AoA and RSS), which give a more dependable placement mechanism. The precision acquired from careful selection of trusted nodes reduces the impact of compromised nodes on the whole localization process.

7.2.4 Computational cost

Figure 6 depicts the computational cost of the different proposed localization techniques. It can be observed that the proposed algorithm JTDSA achieves a 54% lower computational cost than SL, 37% lower cost than SecRET, and 22% lower cost than SALM across various node scenarios. This reduction in computational overhead is primarily due to the efficient trust evaluation mechanisms employed, which minimize the complexity of trust calculations. Additionally, the JTDSA technique utilizes lightweight digital signature algorithms, ensuring that the processing requirements are kept low. The involvement of a limited set of Secondary-anchor Nodes (SNs) in the localization process and the smaller size of the signed MAC also contribute to the overall decrease in computational demands. This efficiency is particularly critical in resource-constrained underwater environments, where both computational and energy resources are limited.

7.2.5 Detection accuracy

It is defined as the accuracy to find out the unauthorized node from the network. Figure 7 illustrates that the JTDSA achieves 5% higher detection accuracy than SL, 3% higher than SecRET, and 2% higher than SALM for different nodes scenario, due to the trust metrics. Moreover, since the localization information is signed by the digital signature scheme, the unauthorized forging of localization information can be easily detected. The JTDSA approach may swiftly detect malicious actions due to its mix of trust metrics and anomaly

Fig. 7 Detection accuracy for nodes

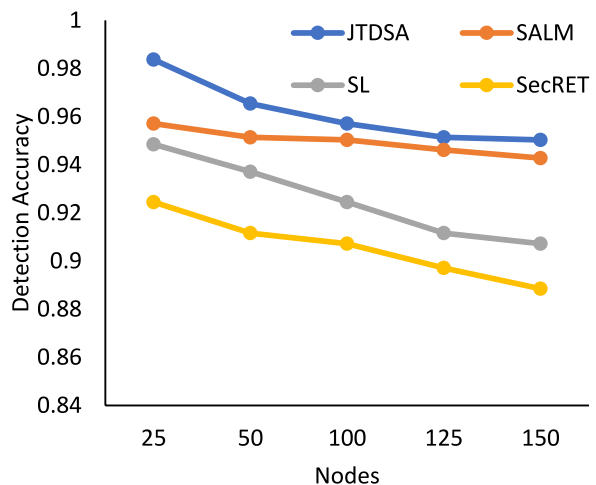


Table 3 Result compared with JTDSA mehtod

Metric	Compared with JTDSA		
	SALM	SL	SecRET
Packet Drop (%)	35% reduction than JTDSA	18% reduction	10% reduction
Residual Energy (%)	36% higher	24% higher	15% higher
Localization Accuracy (%)	99.2% (+4%)	2% higher	3% higher
Computational Cost (%)	54% lower	37% lower	22% lower
Detection Accuracy (%)	5% higher	3% higher	2% higher

detection capabilities. By quicklyssss isolating corrupted nodes, the approach guarantees that overall network integrity is preserved, which strengthens its usefulness in UWSNs.

Furthermore, Table 3 shows the comparative result analysis with other state-of-the-art localization in UWSNs for better understanding.

8 Challenges and future directions

This approach provides a strong solution for safe localization in Underwater Wireless Sensor Networks (UWSNs); yet, it has several drawbacks, especially in large-scale deployments. Scalability is a significant problem, as the trust evaluation procedure can become computationally costly as the number of nodes rises. This may cause delays in both node selection and data processing, reducing the network's overall performance. There is also a difficulty with communication overhead. While digital signatures improve security, they also add to communication needs. In large networks, this additional expense can lead to greater latency and reduced throughput, potentially disrupting effective communication among nodes. The unpredictability of undersea surroundings complicates issues further. Factors such as node mobility and changing environmental circumstances might have an influence on the dependability of trust values. Malicious nodes might exploit these variations, thereby exposing the network's defenses.

Finally, resource restrictions have a substantial impact on the implementation of the JTDSA approach. Underwater sensor nodes frequently have limited battery life and processing capabilities, making it difficult to achieve a compromise between energy conservation and robust security, especially in large-scale installations.

Future advancements to the JTDSA technique's scalability and resilience in underwater deployments might involve creating a distributed trust evaluation system, inventing adaptive digital signature methods, and fine-tuning dynamic trust adjustments for real-time updates. Furthermore, a hierarchical network architecture with energy harvesting methods might improve performance and increase the operational lifespan of sensor nodes in large-scale settings.

9 Conclusion

In this study, we present the Joint Trust-based Detection and Signature-based Authentication (JTDSA) approach for improving safe localization in Underwater Wireless Sensor Networks. This study adds to the theoretical underpinning and practical implementations of wireless sensor networks by addressing important security flaws in previous localization approaches.

The combination of trust-based detection and digital signature authentication provides a powerful solution for mitigating different assaults while maintaining the reliability and accuracy of localization data. The main contribution of this research is the creation of a complete framework that integrates trust evaluation with digital signature techniques. Our technology improves the identification of compromised nodes by using a multi-metric approach to trust evaluation, and the usage of digital signatures protects data integrity throughout transmission.

Furthermore, the hybrid strategy of integrating Angle of Arrival (AoA) and Received Signal Strength (RSS) measures enhances overall localization accuracy, indicating a considerable improvement over previous method. The JTDSA approach has several practical benefits, including a 35% reduction in packet loss rates and improved residual energy in underwater sensor nodes, that promotes more sustainable operations in resource-constrained areas. Furthermore, the capacity to efficiently detect and isolate hostile nodes improves network security, critical for applications including environmental monitoring, catastrophe prevention, and military operations. The lightweight nature of the suggested methods minimizes computational and energy overhead, allowing for efficient implementation in real-world applications. Simulation findings show that JTDSA enhances localization accuracy by 4% over previous approaches, resulting in an overall accuracy of 99.2%. Furthermore, the approach improves attack detection accuracy by 3%, demonstrating that the suggested JTDSA technique is a viable alternative for safe and reliable localization in UWSNs.

Despite its achievements, the JTDSA approach has certain drawbacks. Environmental issues like as acoustic noise and varied undersea conditions can have an impact on trust evaluation efficacy. Future study might look into building a distributed trust management system to improve scalability and reduce single points of failure. Creating adaptive digital signature systems that respond to changing network conditions might increase communication efficiency while retaining security.

Acknowledgements The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number 007.

Authors' contributions All authors are the main authors of the current paper. They contributed to the development of the ideas, design of the study, theory, results analysis, and paper writing, and finally reading and approving the final manuscript.

Funding Not Applicable.

Data availability Data will be made available on reasonable request.

Declarations

Ethical approval Ethical approval is not applicable for this article.

Conflict of interest The authors declare that they have no competing interests.

References

1. Tuna G, Gungor VC (2017) A survey on deployment techniques, localization algorithms, and research challenges for underwater acoustic sensor networks. *Int J Commun Syst* 30(17):e3350
2. Shanthi MB, Anvekar DK (2018) Secure localization for underwater wireless sensor networks based on a probabilistic approach. In: 2018 IEEE second international conference on advances in electronics, computers, and communications (ICAEECC). Bangalore, India, pp 1–6

3. Shukla V, Kumar A, Bhan V (2018) Minimizing the Energy Consumption Using a Secure Recursive Localization Approach for Distributed Networks in Underwater Acoustic Wireless Sensor Networks. *Int J Sci Res Math Stat Sci* 5(3):153–159
4. Dong M, Li H, Qin Y, Hu Y, Huang H (2024) A secure and accurate localization algorithm for mobile nodes in underwater acoustic network. *Eng Appl Artif Intell* 133:108157
5. Ahmad I, Rahman T, Zeb A, Khan I, Ullah I, Hamam H, Cheikhrouhou O (2021) Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wirel Commun Mob Comput* 2021(1):1444024
6. Li H, He Y, Cheng X, Zhu H, Sun L (2015) Security and privacy in localization for underwater sensor networks. *IEEE Commun Mag* 53(11):56–62
7. Sharma P, Singh RP, Mohammed MA, Shah R, Nedoma J (2021) A survey on holes problem in wireless underground sensor networks. *IEEE Access* 10:7852–7880
8. Yang Y, Wu Y, Yuan H, Khishe M, Mohammadi M (2022) Nodes clustering and multi-hop routing protocol optimization using hybrid chimp optimization and hunger games search algorithms for sustainable energy efficient underwater wireless sensor networks. *Sustain Comput: Inf Syst* 35:100731
9. Kumar A, Kumar P (2023) An improved sparsity-aware normalized least-mean-square scheme for underwater communication. *ETRI J* 45(3):379–393
10. Draz U, Ali T, Ahmad Zafar N, Saeed Alwadie A, Irfan M, Yasin S, ... Khan Khattak MA (2021) Energy efficient watchman-based flooding algorithm for IoT-enabled underwater wireless sensor and actor networks. *ETRI J*, 43(3), 414–426
11. Guqhaiman A, Akanbi O, Aljaedi A, Chow CE (2020) Lightweight multi-factor authentication for underwater wireless sensor networks. In: 2020 IEEE international conference on computational science and computational intelligence (CSCI). Las Vegas, NV, USA, pp 188–194
12. Wang H, Wen Y, Lu Y, Zhao D, Ji C (2019) Secure localization algorithms in wireless sensor networks: a review. *Advances in computer communication and computational sciences: Proceedings of IC4S 2017*, vol 2, pp 543–553
13. Boukerche A, Oliveira HA, Nakamura EF, Loureiro AA (2008) Secure localization algorithms for wireless sensor networks. *IEEE Commun Mag* 46(4):96–101
14. Goyat R, Kumar G, Alazab M, Saha R, Thomas R, Rai MK (2021) A secure localization scheme based on trust assessment for WSNs using blockchain technology. *Futur Gener Comput Syst* 125:221–231
15. Svendsen B, Kadry S (2024) A dataset for recognition of norwegian sign language. *International Journal of Mathematics, Statistics, and Computer Science* 2. <https://doi.org/10.59543/ijmscs.v2i.8049>
16. Nguyen TN, Le VV, Chu SI, Liu BH, Hsu YC (2022) Secure localization algorithms against localization attacks in wireless sensor networks. *Wirel Pers Commun* 127:767–792. <https://doi.org/10.1007/s11277-021-08404-4>
17. Han G, Liu L, Jiang J, Shu L, Rodrigues JJ (2016) A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks. *Sensors* 16(2):229
18. Shanthi MB, Anvekar DK (2019) Secure localization in UWSN using combined approach of PSO and GD methods. *J Recent Technol Eng* 7:1535–1538
19. Hu X, Tan W, Yan J, Ma C (2020) Security and improvement of aggregate signature scheme for underwater wireless sensor networks and certificateless aggregate signature scheme for vehicular ad hoc networks. In: 2020 IEEE 5th international conference on mechanical, control and computer engineering (ICMCCE). Harbin, China, pp 574–577
20. Yan J, Meng Y, Yang X, Luo X, Guan X (2020) Privacy-preserving localization for underwater sensor networks via deep reinforcement learning. *IEEE Trans Inf Forensics Secur* 16:1880–1895
21. Elhoseny M, Lakhan A, Rashid A, Mohammed M, Abdulkareem K (2022) Underwater Sensor Multi-Parameter Scheduling for Heterogenous Computing Nodes. *ACM Trans Sensor Networks (TOSN)* 18(3):1–23
22. Misra S, Ojha T (2021) SecRET: secure range-based localization with evidence theory for underwater sensor networks. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 15(1):1–26. <https://doi.org/10.1145/3431390>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

Manni Kumar¹ · Nitin Goyal² · Ramy Mohammed Aiesh Qaisi³ · Mohd Najim³ · Sachin Kumar Gupta⁴

✉ Sachin Kumar Gupta
sachin.ece@cuajammu.ac.in

Manni Kumar
mannikumar55@gmail.com

Nitin Goyal
dr.nitingoyal30@gmail.com

Ramy Mohammed Aiesh Qaisi
dgaisi@uj.edu.sa

Mohd Najim
mngalib@uj.edu.sa

¹ Department of Computer Science & Engineering, Chandigarh University, Gharuan, Punjab, India

² Department of Computer Science Engineering, School of Engineering and Technology, Central University of Haryana, Mahendergarh, Haryana 123031, India

³ Department of Electrical and Electronic Engineering, College of Engineering, University of Jeddah, Jeddah 21589, Saudi Arabia

⁴ Department of Electronics and Communication Engineering, Central University of Jammu, Jammu 181143, UT of J&K, India