yuvakṣhētṛa®
Institute of Management Studies (YIMS)
Ezhakkad, Mundur, Palakkad - 678631, Kerala.
ACCREDITED BY NAAC WITH B+ GRADE (1st CYCLE)
Affiliated to the University of Calicut & Managed by the Diocese of Palghat

DEPARTMENT OF COMPUTER SCIENCE

ICACRI

INTERNATIONAL CONFERENCE FOR ADVANCED COMPUTATIONAL RESEARCH AND INNOVATIONS

2024

VOLUME I , ISSUE I

CONFERENCE PROCEEDINGS

English Language

Title of the Book	: International Conference for Advanced Computational Research and Innovations (ICACRI - 2024)
Editor	: JIBIN JOY
Published by	: Yuvakshetra Institute of Management Studies
Address	: Ezhakkad, Mundur, Palakkad, 678600
Rights Reserved	
First Edition	: FEBRUARY 2024
Cover Design	: JIBIN JOY
Printed at	: Jim Offset, Palakkad
Publishers	: Yuvakshetra Publications, Ezhakkad, P.O, Mundur, Palakkad
E mail	: yimspublication@yuvakshetra.org,
	: yuvakshetra@gmail.com
Website	: www.yuvakshretra.org
Tel	: 9400012368, 8714345789
Distributors	: Yuvakshetra Publications, Ezhakkad, P.O, Mundur, Palakkad
E mail	: yimspublication@yuvakshetra.org,
	: yuvakshetra@gmail.com

ISBN : 978-81-968246-5-5.

CVDS - CONNECTIVITY BASED VOID DETECTION AND OPTIMIZED SECURE ROUTING IN UNDERWATER SENSOR NETWORK

Author 1:

DEEPTHI B P
PHD SCHOLAR
DEPARTMENT OF COMPUTER SCIENCE
SRI KRISHNA ARTS AND SCIENCE COLLEGE
COIMBATORE
deeptham08@gmail.com

Author 2:

Dr.J.LEKHA
ASSOCIATE PROFESSOR
DEPARTMENT OF DATA SCIENCE
CHRIST (Deemed to be University)
Lavasa Campus,Pune.
lekha.j@christuniversity.in

ABSTRACT

In the realm of underwater sensor networks, the process of transmitting packets from a source to a destination presents a multitude of requirements and challenges. Key considerations encompass neighbour detection, path maintenance, void region resolution, and the establishment of secure communications. The network's dynamic nature often leads to frequent disconnections, making it crucial to devise effective strategies. The proposed CVDS - Connectivity-based void detection and optimum secure routing method for underwater sensors primarily centres on path formation via hop routing. In situations where a node finds itself within a void region, the mobile sink is dispatched to retrieve the packets before their onward delivery to the destination. Moreover, each node diligently evaluates the trustworthiness of potential neighbours before selecting them as forwarders, ensuring secure data transmission. The implementation of this approach has led to notable improvements in network performance, particularly in terms of enhanced throughput and minimized delays. These enhancements underscore the efficacy of the proposed method, which addresses critical challenges in underwater sensor network communication and routing.

Keywords: Neighbour Detection; Void region; Mobile Sink; Trusted forwarder; Secure Transmission;

1 INTRODUCTION

Wireless sensor networks find extensive applications in remote monitoring and event detection across diverse domains. These include human body monitoring, environmental surveillance, tracking product activations, and monitoring underwater variations. These networks prove particularly valuable in critical and remote regions, where changes and events are tracked through an array of strategically placed sensors.

Within this network, sensors are equipped to sense, transmit, and receive data packets. While the network primarily operates over the acoustic channel, it leverages wireless channels above the sea to establish connections due to the uncertainties involved. However, the network faces challenges such as energy depletion, link failures, the emergence of void regions, and security vulnerabilities. These issues often lead to packet losses and frequent network disconnections, resulting in fluctuating network performance and occasional failures.

These challenges are dynamic and evolve over time, necessitating adaptive strategies to mitigate their impact on network reliability and effectiveness.

The uncertainties inherent in the underwater environment pose significant challenges for sensors within the network. It's crucial for the source node, intermediate sensors, and the ultimate destination to maintain continuous connectivity throughout the data transmission process. This seamless connection is pivotal for enhancing network performance and resource efficiency.

However, the network faces various threats, including potential attacks that can disrupt communication, resulting in the loss or interruption of network connections and capabilities. These disruptions not only deplete network resources but also elevate the risk of network failures. In cases where nodes become compromised or unreliable, network activities can come to a halt, further underscoring the importance of robust strategies and security measures to sustain network functionality.

The integrity of original data within the network can be compromised due to several factors, including data fluctuations, malicious activities, and the dynamic nature of nodes. Moreover, packets may undergo alterations or even fail to reach their intended destinations when malicious nodes interfere. Such disruptions can escalate into urgent situations if data is not delivered promptly, underscoring the critical need for the network to function flawlessly.

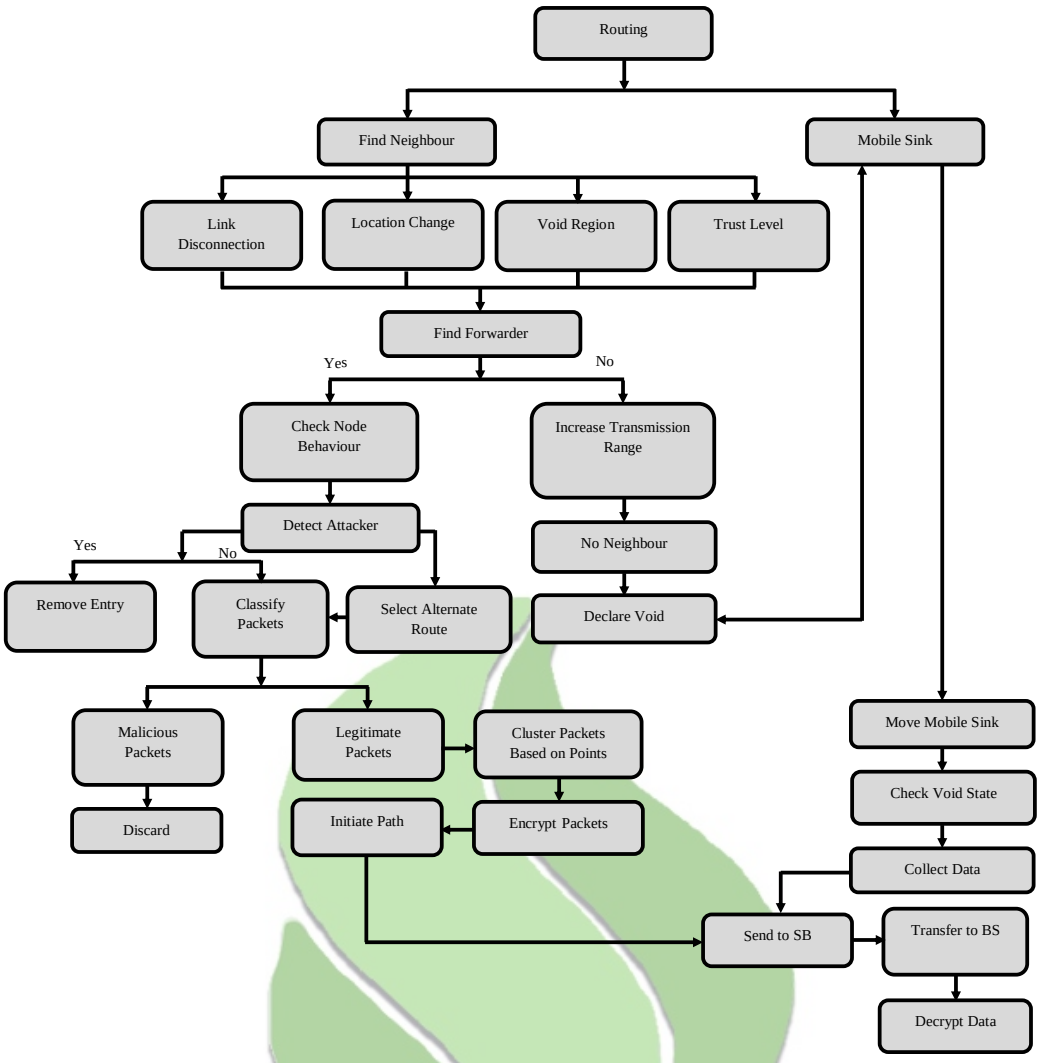
Timely detection of malicious nodes is imperative, and measures must be in place to ensure that trapped packets can find alternate routes for successful transmission. This proactive approach is essential to maintain the network's operational efficiency and reliability while safeguarding against potential disruptions and urgent scenarios.

In addition to addressing issues related to malicious nodes and data disruption, the network must also have mechanisms in place to detect and manage void regions effectively. One approach to tackle this challenge involves collecting data via a mobile sink to prevent packet loss before it reaches the final destination. Subsequently, the data is subjected to classification using fuzzy optimization techniques, distinguishing between harmful and normal data.

Within the proposed CVDS framework, the network performs a range of critical tasks, including neighbor detection, path establishment, destination updates, security validations, link monitoring, void region surveillance, and mobile sink call requests, among others. This multifaceted approach is pivotal in enhancing network performance by facilitating cooperative interactions among sensors, destinations, and mobile sinks, as depicted in Figure 1.1. These collaborative efforts collectively contribute to the improved efficiency and reliability of the network.

Figure.1.1 Route Selection

The remainder of this paper is organized as follows to provide a comprehensive understanding of the study's context and findings. In Section 2, we delve into related work that is pertinent to the scope of this research. Section 3 then outlines the development of the proposed method, CVDS-Connectivity, which addresses void detection and secure routing within an underwater sensor network. We illustrate the robustness of our proposed method through graphical representations. Lastly, in Section 5, we conclude the paper by outlining potential avenues for future research and exploration in this field



2 RELATED WORKS

Efficient and timely routing and broadcasting of packets from the underwater sensor nodes to the surface is of crucial importance for connecting these applications to the land internet. Acoustic waves are used in underwater acoustic sensor network as the best alternative for the severely attenuated radio waves in water medium [19]. Underwater Sensor Networks and their ground information counterparts require the development of efficient algorithms, reliable security mechanisms and the entire involvement of node routing information while maintaining a correct and effective transmission of data, which increases the network lifecycle are essential when routing protocols for Underwater Sensor Networks [1]. Underwater wireless sensor networks are made up of nodes deployed both on the underwater and surface of the water. All nodes must communicate and share data with other devices in the same network and the ground station. Sensor network communication methods feature data transmission via acoustic, electromagnetic, or optical wave mediums [3]. These works together with these Remotely Operated Vehicles, which are controlled from the ship, or Autonomous Underwater Vehicles, that can autonomously navigate the deep waters are based on some set of instructions. The ROVs/AUVs, sensors and anchors collect and feed information from the seabed. These can measure parameters such as foundation strength and mooring tensions [7]. The underwater sensor design in such applications ranges from simple to complex. This underwater wireless sensor networks research area is very challenging, and most work that has been conducted using terrestrial wireless sensor networks cannot be directly implemented into underwater wireless sensor networks because different communication channels are used and the characteristics of underwater environments are unique [14]. We describe key technical issues and new research approaches that come from revising traditional assumptions and exploiting

cross-layer optimization both between adjacent layers and throughout the entire protocol stack, from the application to the physical link. We also describe the currently available hardware, and discuss tools for modeling and simulation, as well as test-beds [2]. Underwater Sensor Networks can be utilized in any scenario from underwater warfare to the monitoring of environmental conditions. Underwater Sensor Networks face constraints like limited bandwidth, high propagation delay, 3D topology, and power constraints. Radio and optical waves are not feasible for communication at each point of ocean [5]. There are many research is under process related to security issue and it is a challenging task due to special constraints of underwater environment because the nodes have limited battery power and limited bandwidth. Therefore, security services help to improve the network life and protect the useful information [15]. Underwater sensor nodes are extremely limited in hardware resources, including energy, computational capability and storage space. Due to higher distances and to more complex signal processing at the receivers to compensate for the attenuation of the signal, the power consumed for underwater acoustic communication is much higher than in terrestrial radio communication [18]. UWSNs are composed of mobile or stationery nodes that collect data using onboard sensors and communicate via low frequency acoustic signals. The sensor nodes collect and transmit sensory data to buoyant gateway nodes which in turn relay the data to the nearest coastal remote station. There has been an increasing interest in monitoring the underwater environment for scientific, industrial and military purposes, and as such the popularity of UWSN [6]. Underwater wireless sensor networks can be divided into deep water and shallow water. Underwater wireless sensor networks routing protocols further can be classified based on communication as acoustic communication, radio wave communication and optical communication. Underwater optical communication has a strong information-carrying capacity and can form a large-capacity wireless communication link [9]. Ultra-lightweight encryption schema evolved which encrypts the contents of communication in UWASN. It provides integrity and confidentiality in between nodes using less space and provides high security with lower computations. The encryption schema should satisfy challenges of underwater like it should be adoptable for underwater transmission, lower computation with less overhead, cost and energy efficient and ensure high security [4]. A wireless sensor network generally has little or no infrastructure. It consists of number of sensor nodes working collectively to monitor an area to obtain data about the environment. The sensor nodes can be deployed in adhoc manner or pre planned manner. In adhoc manner the sensor nodes are deployed randomly into the field and the network is then left unattended to perform monitoring [11]. Underwater sensor nodes in UWSNs cover a definite area of the sea to sense the determine attributes and transfer the information to onshore base station that situated near to the water surface. Consequently, communication systems in the underwater sensor network involve the transmission of data through radio frequency, electromagnetic or optical wave and acoustic medium [17]. The current study presents an algorithm for secure routing in underwater sensor networks to make them resistant against wormhole and Sybil attacks and safely transfer the data from the underwater sensor nodes to the sink node [12]. UWSNs can be applied to monitoring marine activities by monitoring the surrounding environment of the marine organisms through acoustic device networks. To transmit the marine environmental conditions, information from one sensor to another can be accomplished by utilizing TDMA protocols. The obtained data can then be used to develop ecosystem models capable of predicting changes in the underwater environment and changes in climate conditions [8]. Underwater sensors move with water currents, and autonomous underwater vehicles are mobile. Although certain nodes in underwater applications are anchored to the bottom of the ocean, other applications require sensors to be suspended at certain depths or to move freely in the underwater medium [13]. To address the communication restrictions of underwater wireless sensor networks, we discuss all the available ways for communication. A new communication architecture for underwater wireless sensor networks. We evaluate acoustic communication in terms of data transmission rate, energy consumption and transmission time [10]. A group of wireless network of sensors was used for precise analytical monitoring of farm water pollution. Applications have also been developed for trout farming to keep track of water quality in the pools. The chemical composition of the water is monitored for a given period, and an algorithm is deployed to show the input-output information [16].

3 CVDS DESIGN AND IMPLEMENTATION

3.1 Network Model

In a topography-rich environment, a network has been established, comprising an array of sensors denoted as S, ranging from (s_1,.. s_5,.., s_n), along with a strategically placed sonobuoy S_B and a central base station B_S. The size of this network can vary depending on its requirements. Each sensor plays an essential role by fostering connections with its neighbouring nodes through regular announcements and upkeep of a neighbour list. These announcements encompass critical information such as the node's precise location (L), its current energy level (E), a timestamp (t), and a trust rating reflective of the node's integrity. Upon receiving announcements from their neighboursN_B, sensors promptly refresh their respective lists.

To bolster the security of communication between the sensors and the B_S, a robust cryptographic system has been implemented. This system leverages elliptic curve-based asymmetric secret keys to facilitate data encryption and decryption, hence classified as a public key cryptography system. Within this framework, two essential keys are employed: the public key (P_{UK}) and the private key (P_K). These keys are instrumental in securing data packets. In particular, a random number (R_N) within the range of 0 to 1, representing elliptic curve points denoted as C_p, is utilized. The P_K is then generated randomly within the specified range encompassing $C_p$and R_N. Consequently, a shared secret key (S_{SK}) is derived.

It is imperative to note that the values C_p and R_N persist throughout each communication session. As a result, the sensors embark on the process of creating new keys for every data transfer, ensuring an added layer of security in this intricate network ecosystem.

$$Gnerate\ P_K \leftarrow Random(C_p, R_N)$$
$$P_{UK} \leftarrow (P_K\ R_{N)}$$
$$S_{SK} \leftarrow P_K + P_{UK}$$

Upon receiving an announcement from its neighbouring node, the sensor immediately initiates a computation process to determine the distance between the node and N_B, denoted as D_{ist}. This distance calculation serves as a significant metric in assessing the spatial relationship between the sensor and its neighbouring node.

$$D_{ist} = \sqrt{(X_1 - X_2)^2 + (Y_1 - Y_2)^2(Z_1 - Z_2)^2}$$

Utilizing the Pythagorean Theorem, the network calculates three distinct positional distances based on the coordinates provided: X_1, Y_1, Z_1 for one point and X_2, Y_2, Z_2 for another. These calculations are pivotal in updating the local distance metric, refining the sensor's address information, and determining the count for the next hop in the network. In essence, this mathematical approach facilitates the precise assessment of spatial relationships and aids in the efficient routing of data within the sensor network.

3.2 Device Communication

In the underwater UW sensor network, connections may be severed due to various factors such as link failures, energy depletion, loss of trust, or changes in mobility. To maintain the network's robustness and ensure uninterrupted communication, through regular updates from N_B play a significant role in preserving link integrity.

The B_S, broadcasts a BS-announcement, which is received by the sonobuoy,S_B. Upon reception of BS-announcement, $S_B$updates information, including the B_S's ID and its location L. Subsequently, S_B disseminates a SB-notification to both the sensors and mobile sinks (M_S), to

effectively establishing and maintaining connections. This SB-announcement is further updated and relayed to neighbouring nodes as part of the network's connection self-healing mechanism.

During data transmissions, UW-sensors multitask by serving as both sensing nodes and routers. This dual role ensures efficient data routing and connectivity within the network. Importantly, the secret shared key, which underpins secure communication, is designed to be shared openly among the legitimate nodes, enhancing the network's overall security posture.

In the process of constructing a viable communication path, each UW-sensor within the network is tasked with the continuous updating of its neighbouring nodes. Several factors come into play when selecting these neighbours, including the nodes' energy levels, signal-to-noise ratios, proximity to the S_B, and their respective trust levels. The sensors themselves introduce noise into the system, both through their devices and the communication channel, necessitating the utilization of multiple pathways for sending and receiving data packets. As an additional layer of complexity, the received signal intensity is carefully calculated during sensor transmissions.

However, the inherent challenge lies in the adverse impact of uncontrollable contaminants generated during communication, which can severely strain the relationships between neighbouring nodes. To mitigate these concerns and bolster security, a range of significant security metrics must be safeguarded against potential attackers. This concerted effort serves to enhance the trustworthiness of the nodes along the communication path.

In the quest for constructing a path towards the S_B, each sensor diligently searches for a qualified S_B in an upward direction. The chosen $S_B$must meet specific criteria: it should not reside in a void region (V_R), and it must possess a trusted node status. This stringent selection process ensures the reliability and security of the path as it advances toward the ultimate destination, the S_B.

In scenarios where a sensor finds itself within the V_R and cannot identify any nearby N_B in close proximity to the destination, it takes an alternative approach. In this situation, the sensor establishes contact with the mobile sink, denoted as M_S, to gather the required data. To facilitate this communication, the sensor has the capability to extend its adjustable transmission range, T_R, based on the detection of the N_B. This extended range enables the sensor to send continuous help request (H_R) messages as broadcast to any direction N_B or M_S, as requesting assistance.

Given the presence of malicious nodes within the network, it becomes imperative to secure the H_R packets to prevent interception or interference by these malicious entities. To achieve this, the H_R message is encrypted (E_{nc}) before being broadcast in the open environment. This encryption step serves as a significant defence mechanism against potential malicious activities within the network, bolstering its overall security.

To establish secure communication channels, legitimate nodes collaboratively generate a secret shared key, denoted as s_{SK}, with their neighbouring nodes and the intended destination. Despite being shared publicly, this shared secret key s_{SK} is instrumental in forming secure connections between sensors. Subsequently, the receiving node decrypts (D_{ec}) the message and proceeds to forward it to the mobile sink, ensuring that the data reaches its intended destination reliably and securely.

Check Sensor L located V_R
If no N_B *within* T_R
Send H_R*Message*
Generate s_{SK}

$$E_{nc} = (S_{SK} + H_R)$$
$$D_{ec} = H_R, s_{SK}$$

In the context of this communication framework, S_{ig} represents the location of the signal sender node, while S_X, S_Y, and S_Z represent the locations of the sensors in the network. It's essential to address the challenge posed by malicious nodes, which emit false noise in the vicinity of legitimate sensors, potentially disrupting the network's operation.

To ensure physical layer confidentiality and the secure operation of sensor resources such as energy, channel selection, and neighbour selection, a verification process is employed. This process assesses the legitimacy of the sender node by considering various features, including noise levels, signal strength, and energy metrics. These criteria help to distinguish between genuine and potentially harmful nodes within the network. Additionally, D_A denotes the dashed node radius, which is determined based on signal information, while C_C represents the coverage centre of the node. D_{ID} corresponds to the dashed node ID, and N_H represents the new hop in the network topology.

When a node from the set of sensors ($s_i \in T_R$) transmits a signal, it does so within a coverage area that is either within the dashed region or in close proximity to the adjustable T_R, with the connected centre at C_C. If the distance to a neighbouring node exceeds the T_R threshold, it is deemed unsuitable for communication within this specific region. This approach helps ensure that nodes are effectively communicating within their designated coverage areas, enhancing the efficiency and reliability of the network, while also safeguarding against potential threats posed by malicious nodes.

$$If\ N_B > 1$$
$$Check\ minimum\ D_{ist} \rightarrow N_B$$
$$D_1 = D_{ist}(S_{IG1X}, S_{IG1Y}, S_{IG1Z}), S_X, S_Y.S_Z$$
$$D_2 = D_{ist}(S_{IG2X}, S_{IG2Y}, S_{IG2Z}), S_X, S_Y.S_Z$$
$$R = \frac{D_1 + D_2}{2}$$
$$Check\ R > T_R$$
$$D_A = \frac{R}{2}$$
$$C_C = \sqrt{R^2}$$
$$If\ N_B \rightarrow D_{ist} < D_A || N_B \rightarrow D_{ist} < C_C$$
$$If\ N_B = S_{IG1}, S_{IG2} \rightarrow Enable\ Signal\ transmission$$
$$If\ N_B \rightarrow D_{ist} > C_C$$
$$D_{ID} = N_B$$
$$N_H = D_{ID}$$
$$N_H = S_{IG2}\ or\ S_{IG1}$$
$$N_B \rightarrow D_{ist} > R\ \ Declare\ I_R$$

Subsequently, the network protocol involves the identification of neighbouring nodes in proximity to the dashed node, followed by an assessment of the incorrect boundary limit, denoted as I_R. The task is to validate whether the node has been contaminated or compromised during signal transmission. This validation process hinges on the observation of whether the signal has ceased within the dashed node radius, D_A. By monitoring the signal's behaviour in this context, the network can discern whether any anomalies or intrusions have occurred, thus enhancing its security and reliability measures.

$$If\ D_{ist} > D_A\ and D_{ist} < T_R$$
$$S_{IG}\ Terminated$$
$$if\ N_B \rightarrow D_{ist} < R_1 || N_B \rightarrow D_{ist} < R_2$$
$$Node\ placed\ near\ D_A$$

3.3 Parameter Validations

To validate the contamination of sensors, the protocol involves modifying both the data list, denoted as D_L, and the node list. These lists contain crucial information, including the identifiers 'i' and 'j' that correspond to specific nodes. The protocol proceeds by aggregating the total data, denoted as T_D, transported between these nodes. Concurrently, packet counts,

represented as P_C, are updated to reflect the recent data transmissions. Subsequently, the average count of data, denoted as A_D, transmitted between nodes is computed and serves as a key metric in assessing network performance. The node list is then updated accordingly to reflect these changes.

Furthermore, the process involves the formation of data groups, referred to as D_G, and the computation of data differences (D_D), variance, and the standard deviation radius, known as D_{PR}. Additionally, it provides information about intra-data group distances while continuously updating the intra-distance metric, denoted as I_D. This continuous tracking of I_D facilitates the identification of the centre point within the data.

Overall, this comprehensive approach enables the network to assess the integrity of its sensor nodes, monitor data exchanges, and maintain data groupings, ultimately contributing to the efficient and secure operation of the sensor network. In this intricate data analysis process, various calculations and assessments are conducted to gain valuable insights. Initially, the maximum data value, denoted as M_P, is determined to locate the midpoint (M) within the data group (D_G). The network then computes the average weight (A_W) value for this data group, assigning weights (w) within the range of 0 to A_W. Additionally, factors such as routing weight (W_R), the affected region (A_R) by malicious packets, and V_R ons come into play.

The next step involves establishing the lower boundary (L_B) and uppermost boundary (U_B) of the affected region (A_R). Furthermore, the network calculates the average of the lesser values (A_L) and the uppermost boundaries (A_U) within this affected region. To manage the weight values, the summation of weight values (S_W) is computed to determine the last data group's weight value (W_{LG}). Additionally, the process involves identifying the maximum membership value (F_M). Data value distances (D_{PD}) are assessed, and intra-group counts (I_C) are updated accordingly.

Further analysis entails the determination of intra-group distances, which are tracked and updated. A similar approach is followed for inter-group counts and distances, enabling the network to gain a comprehensive understanding of data relationships and patterns. These calculations and assessments play a pivotal role in deciphering complex data dynamics within the network, aiding in decision-making processes and enhancing overall network efficiency and reliability.

.

$$T_D = \sum D_T$$

$$A_D = \frac{T_D}{P_C}$$

$$D_D = (T_D - A_D)^2$$

$$D_{PR} = \frac{S_{TD}}{\pi}$$

$$If\ D_D < D_{PR} \rightarrow Update\ P_C\ and\ M_P$$

$$D_{D1} = T_D - M_P$$

$$D_{D1} < R_R \rightarrow Remove\ data\ from\ D_T$$

$$If\ \ D_G > 1\ \ find\ objective\ O_F$$

$$A_W = \frac{1}{D_G}$$

$$w = (0, A_W)$$

$$S_W = S_W \pm w$$

$$W_{LG} = 1 - S_W$$

$$K = A_D{}^{\mathrm{m}}(D_{PR} - T_D)^2$$

$$O_F = O_F \pm K$$

$$F_M \leftarrow member \pm w^m(D_{PR} - T_D)^2$$

$$Update\ maximum\ F_M$$

$$A_R = \sqrt{\frac{1}{T_D sum}}$$

$$L_B \pm T_D - A_R$$

$$U_B \pm T_D + A_R$$
$$A_L = \frac{L_B}{T_D}$$
$$A_U = \frac{U_B}{T_D}$$
$$D_{PD} = T_D - M$$
$$I_D = I_D \pm I_C - M$$

When the data group consists of more than one element, the protocol proceeds to perform a series of important computations and updates. These calculations include determining and updating the normal data count, as well as computing the average data group (A_{VGD}).

Additionally, the protocol calculates the difference and the sum of differences in data variations, referred to as D_{DS}, and computes the data variance, known as D_V, along with the standard deviation of the data, represented as S_{TDD}.

These calculations play a crucial role in assessing the statistical properties and variations present within the data group, facilitating a more in-depth comprehension of the dataset's behaviour and distribution patterns. By continuously updating these metrics, the network protocol is empowered to make well-informed decisions and necessary adjustments, guided by the observed data patterns and variations. This systematic approach serves to bolster the overall performance and reliability of the network, ensuring its efficient operation in handling the data at hand.

$$A_{vgd} = \frac{N_D}{D_G}$$
$$D_{DS} = (A_{vgd} - M)^2$$
$$D_v = \frac{D_{DS}}{D_G}$$
$$S_{TDD} = \sqrt{D_v}$$

Following the aforementioned computations, the protocol proceeds to determine the lesser boundary of data deviation, denoted as L_{BD}, as well as the uppermost boundary, referred to as U_{BD}. Additionally, it identifies and isolates malicious packets within the dataset, labelled as P_M. When a node is responsible for transmitting such malicious packets, the protocol updates the count associated with them. Subsequently, it identifies the specific node responsible for transmitting these malicious packets based on their node ID and subsequently enforces the action of dropping these flagged packets. This meticulous process ensures the detection and containment of malicious activity within the network, safeguarding its integrity and security.

$$L_{BD} = D_{DS} - S_{TDD} - D_{PR}$$
$$U_{BD} = D_{DS} + S_{TDD} + D_{PR}$$
$$P_M = \frac{T_D < L_{BD}}{2} || T_D > U_{BD}$$

3.4 Forwarder Selection

If the condition is not satisfied enable hop-based forwarding.

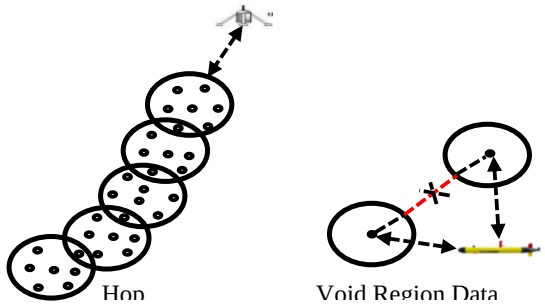


Figure 3.4.1 Data Transmission

In the network infrastructure, when a sensor node identifies a next-hop forwarder leading towards the ultimate destination, it promptly updates its routing information accordingly, as depicted in Figure 3.4.1. In cases where there are multiple available next-hop options, the protocol performs calculations to determine the shortest distance, ensuring efficient data routing. Consequently, the protocol proceeds to update the neighbour nodes with the most current routing information, including neighbour distances and local distances (L_D).

The parameter C_D represents the connected distance within the network, pivotal for establishing efficient routes, and the routing table (R_T) contains vital routing information for reference. Periodically, these routing tables and associated distances are updated to account for dynamic changes in the network topology and to maintain the most optimal paths for data transmission. This continuous monitoring and adjustment process contribute to the network's ability to reliably and efficiently route data towards its intended destination, promoting robust and responsive network performance.

$$C_D = N_B \rightarrow D_{ist} + L_D$$
$$If\ C_D < N_B \rightarrow D_{ist}$$
$$Update\ Forwarder\ and\ R_T$$

In cases where a sensor node has multiple neighbours, the network protocol initiates a series of updates to the R_T and computes the connection probability (C_B) using the following steps. Firstly, a random number denoted as R_N is generated. Subsequently, this random number is utilized to assign weights and compute the average weight for the neighbour counts, known as N_{BC}. Additionally, the protocol calculates the distance probability (D_P) and determines the weighted neighbour (W_N) values.

A crucial step in this process involves computing the maximum neighbour count, labelled as M_N, which is instrumental in selecting the most suitable forwarder among the available neighbours. These calculations and weight assignments collectively serve to optimize the selection of the forwarder node based on various factors, including connection probability, distance, and neighbour counts. This meticulous approach ensures the efficient and reliable routing of data within the network, taking into account dynamic network conditions and topology changes.

$$C_B = \frac{1}{N_{BC}}.$$
$$If\ R_N < C_B \rightarrow Update\ random\ Probability$$
$$D_P = \frac{1}{1 + D_{ist}}$$
$$W_N = wD_P$$
$$M_N = \frac{N_B}{N_{BC}}$$

To maintain the vitality of the link, it's imperative to periodically update both the forwarder's distance and the next-hop node in the network. This routine updating ensures that the connection remains current and responsive. In cases where the link faces disruption due to disconnection events or malicious activities, it becomes crucial to swiftly reroute packets through an alternative neighbour. To achieve this, the network continuously updates the connection distances, enabling it to quickly identify and establish new viable paths for data transmission. This dynamic approach ensures the network's resilience, even in the face of challenges, by swiftly adapting and rerouting traffic as needed.

$$If\ C_D < N_B \rightarrow D_{ist}\ and\ if\ C_D\ is\ affected$$
$$Divert\ Packets\ and\ renew\ R_T$$

When the R_T does not contain the destination address, the network protocol initiates sidestep routing, denoted as S_S routing. However, if the destination address is present in the routing table,

the protocol proceeds to inspect the most recently received packets for any potential malicious content. These packets undergo encryption, incorporating crucial node metrics such as node N_{ID}, t, E_{nc}.

The protocol then considers the packet interval (P_I), current time (C_T), and the last received packets (L_p) to identify any signs of malicious activity within the network. If a node detects malicious packets through the enclosed metrics, it takes swift action. Specifically, it notifies the sender node about the identified malicious content and disseminates a malicious notification throughout the network. This proactive approach aids in promptly addressing and mitigating potential security threats, maintaining the network's integrity and security.

$$S_S = L_p + P_I < C_T$$

$$L_p = C_T + P_I$$

$$E_{nc} = (M + S_{SK})$$

To uncover any void zones within the network, each node diligently keeps its distance metrics between neighbours, assesses available forwarder options, and continuously updates the linked distances. This regular maintenance ensures that the network remains informed about the spatial relationships and connectivity status among nodes. As the data list gets populated with data counts, the protocol proceeds to determine the perceived transmission range for each node. This range takes into account various factors and metrics to provide an accurate assessment of the node's transmission capabilities within the network.

Ultimately, this meticulous process ensures that data packets are effectively routed and transmitted to their intended destination. By maintaining up-to-date distance information and optimizing the transmission ranges, the network strives to achieve efficient and reliable data delivery throughout its entire operational scope

.

$$V_D = B_B \rightarrow D_{ist} > T_R \; at \; C_T$$

4 RESULTS AND DISCUSSION

The proposed CVDS-Connectivity-based method represents a significant advancement in addressing the complex challenges of underwater sensor networks. By focusing on critical aspects such as path formation, void region resolution, and secure communication, this approach enhances network performance given as Table 4.1 on multiple fronts. Through the utilization of hop routing and the strategic deployment of mobile sinks, it effectively tackles network disconnections and packet loss in void regions. Additionally, the trust-based neighbour selection and data encryption bolster network security. The outcomes are tangible, with improvements in packet delivery ratio, throughput and minimal delay, packet drops ensuring more efficient and reliable data transmission within underwater environments. This method demonstrates promising potential for enhancing the effectiveness and resilience of underwater sensor networks in various monitoring and surveillance applications.

CVDS	
Simulation Parameters	Value
Channel type	UnderwaterChannel
Radio-propagation model	Propagation/UnderwaterPropagation
MAC type	Mac/UnderwaterMac/BroadcastMac
Antenna model	Antenna/OmniAntenna
Maximum Queue Length	50
Routing protocol	CVDS

Number of Node	100
X dimension of topography	500
Y dimension of topography	500
Simulation Time	200
Initial energy in Joules	100
Packet Interval	5
Packet-size	512 bytes
Receiving Power	0.75
Transmission Power	2.0

Table 4.1 Simulation Parameter

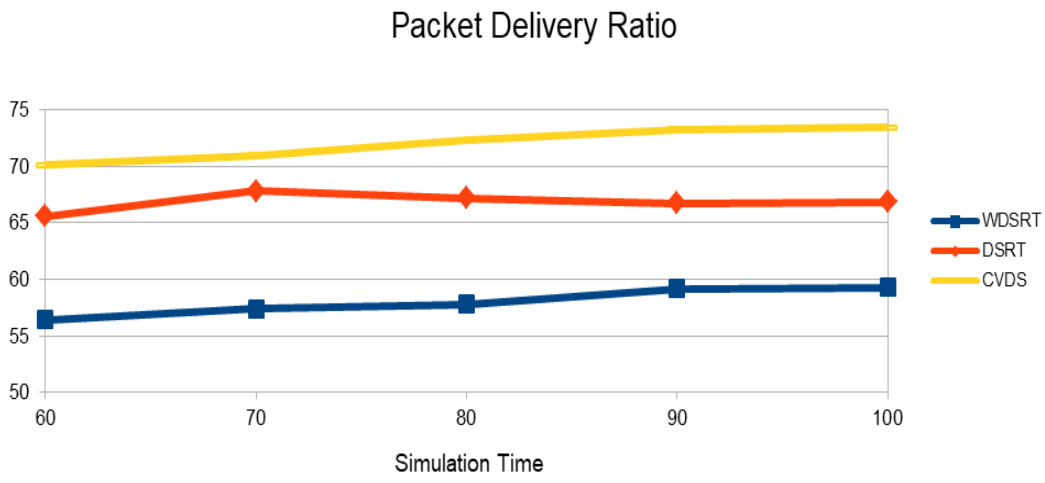


Figure.4.1. Simulation Time Vs Packet Delivery Ratio

In Figure 4.1, the performance of packet delivery ratios for CVDS and DSRT, along with basic underwater protocols, is visually represented. To calculate the received packet ratio, we compute the percentage of packets received by the destination from both the source and other intermediate nodes. In this assessment, it becomes evident that CVDS surpasses the other examined protocols, showcasing its superior performance in packet delivery. The proposed method implemented in CVDS takes a dynamic approach to path selection, adapting to the underwater environment. This adaptability ensures that packets reach their destination more efficiently. Depending on the specific network conditions, the protocol alternates between hop-based path selection and mobile sink-based path selection, tailoring its strategy to the prevailing situation. Moreover, the protocol places a strong emphasis on security metrics, rigorously

evaluating them before selecting a forwarder for data transmission.

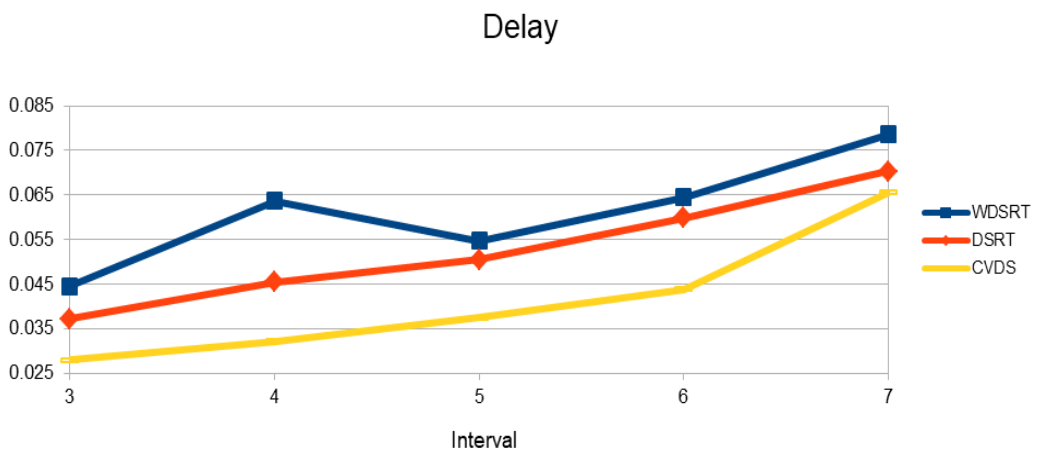


Figure.4.2. Interval Vs Delay

Figure 4.2, provides an insightful comparison of transmission delays between the proposed CVDS protocol and existing protocols. Notably, CVDS emerges as the frontrunner, exhibiting the shortest transmission delay among the protocols under examination. This delay encompasses various components, including propagation delay, queuing delay, and path stability delay. It's essential to note that in underwater networks, path stability and transmission conditions can fluctuate, leading to variations in node queues and consequently, affecting the overall transmission delay. The CVDS protocol takes a proactive approach to address these challenges by prioritizing path selection strategies during both normal and void states. Moreover, it places a strong emphasis on the secure selection of forwarders for data transmission.

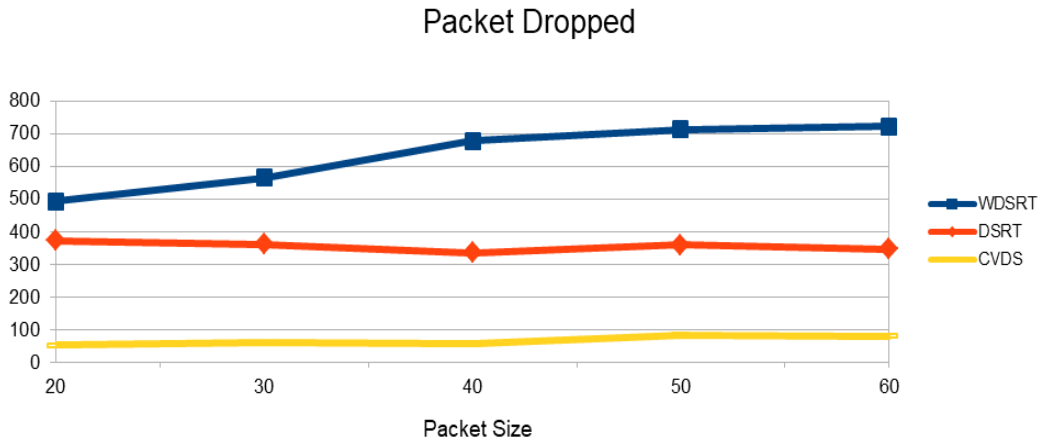


Figure.4.3. Packet Size Vs Packet Dropped

The occurrence of packet drops in the network can be attributed to various factors, including path disconnections, void states within the network, and potentially malicious behaviour

exhibited by certain forwarders. In the case of CVDS, a protocol meticulously designed to address these challenges, the performance in terms of packet loss is notably minimized, as demonstrated in Figure 4.3. This achievement is primarily due to the protocol's strategic emphasis on path selection, with a focus on both hop routing and mobile sink routing. When a node finds itself in a void region, the mobile sink efficiently collects data in an encrypted format. Furthermore, should additional packets enter the network, hop routing is employed to ensure their reliable delivery to the intended destination.

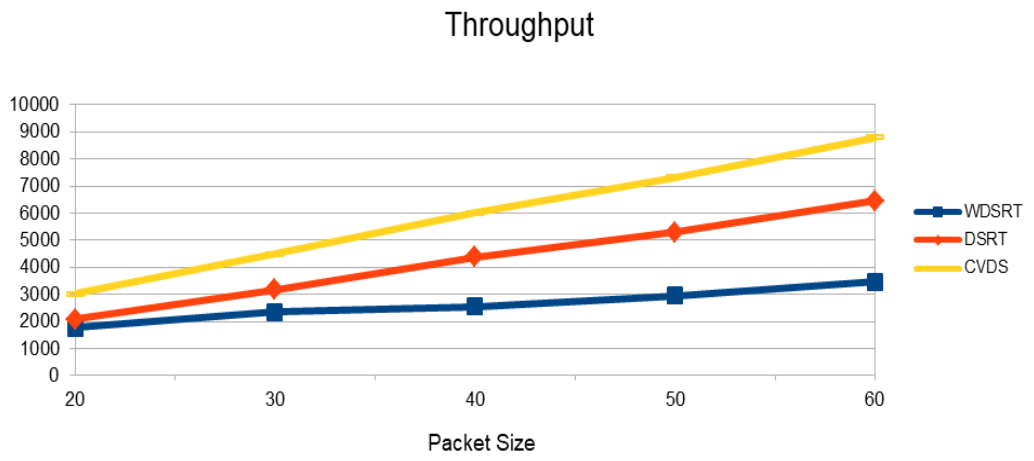


Figure.4.4. Packet Size Vs Throughput

The proposed CVDS protocol has demonstrated superior performance when it comes to throughput compared to other protocols. Throughput is calculated based on the quantity of packet bits successfully delivered to the destination. When the destination receives a higher volume of packet bits, it signifies the protocol's effectiveness and excellent performance, as evidenced in Figure 4.4. This notable improvement in throughput can be attributed to several key factors. Firstly, the protocol prioritizes link stability, ensuring a consistent and reliable connection between nodes. Additionally, it places a strong emphasis on secure data transmission, which further enhances network performance. These combined efforts contribute to the increased quantity of successfully delivered packet bits, ultimately resulting in improved network throughput and overall data transfer efficiency.

Conclusion

In conclusion, the network operation involves various critical processes to ensure efficient data transmission and security. Path distance is a fundamental metric, guiding sensor nodes in choosing neighbors or the mobile sink for packet forwarding. In cases where nodes find themselves without suitable neighbors, referred to as void nodes, they establish secure communication with the mobile sink for packet transfer. Each node operates within its transmission range, carefully selecting communication partners while actively monitoring for malicious activity. Any nodes operating outside their coverage area undergo validation for incorrect borders and adjustments. During sensing periods, data integrity is meticulously checked, and the data list is updated. Using this data list, nodes identify average data values, construct data groups, and ascertain deviations. They also determine the lowest and highest data value groups and their corresponding boundaries. This information is

leveraged to compute data value differences and identify critical and legitimate packets while dropping malicious ones. To handle additional data packets efficiently, hop-based forwarding is simulated when multiple sensors transfer packets simultaneously. In cases where nodes lack forwarders, alternative paths are explored, and the transmission range is extended if necessary. Assistance requests are sent to the mobile sink to recover from void regions. Moreover, connection probabilities are calculated, and weight values are assigned to links. Data packets are transmitted in encrypted form to the destination and decrypted upon arrival. Looking ahead, future network designs may incorporate multichannel capabilities to further enhance packet transfer efficiency. The use of duty cycles, as validated by the MAC layer, can effectively schedule packet transmissions to mitigate channel congestion and interference. These strategies collectively contribute to the network's robustness, security, and overall performance in fulfilling its data transmission objectives.

References

[1] M.Kiranmayi, and Dr. Kathirvel Ayyaswamy, "Underwater Wireless Sensor Networks: Applications, Challenges and Design Issues of the Network Layer -A Review", International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.1, 2015.

[2] John Heidemann, Milica Stojanovic and Michele Zorzi, "Underwater sensor networks: applications, advances and challenges", 2012.

[3] Irfan Ahmad, Taj Rahman, Asim Zeb, Inayat Khan, Inam Ullah, Habib Hamam and Omar Cheikhrouhou, "Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks", Hindawi Wireless Communications and Mobile Computing Volume, 2021.

[4] Kotari Salini and M.B Mukesh Krishnan, "Improvisation of underwater wireless sensor network's efficiency for secure communication", 2nd International conference on Advances in Mechanical Engineering(ICAME), 2018.

[5] Khalid Mahmood Awan, Peer Azmat Shah, Khalid Iqbal, Saira Gillani, Waqas Ahmad, and Yunyoung Nam, "Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges", Hindawi Wireless Communications and Mobile Computing Volume, 2019.

[6] Aliyu Gana Yisa, Tooska Dargahi, Sana Belguith, and Mohammad Hammoudeh, "Security Challenges of Internet of Underwater Things: A Systematic Literature Review", 2021.

[7] S.Prince Sahaya Brighty, Brindha.S.J., and R.HemaGayathri, "Recent Advances and Challenges in Underwater Sensor Networks - Survey", International Journal of Innovations in Engineering and Technology (IJIET), Volume 8 Issue 1 – February 2017.

[8] Mohammad Alsulami, Rafaat Elfouly and Reda Ammar, "Underwater Wireless Sensor Networks: A Review", 11th International Conference on Sensor Networks, 2022.

[9] Shiva Mishra, and Dr. Devesh Katiyar, "A Literature Survey for Underwater Wireless Sensor Networks", International Conference on Intelligent Technologies & Science(ICITS), 2022.

[10] Seema Verma, and Prachi, "Communication Architecture for Underwater Wireless Sensor Network", I. J. Computer Network and Information Security, 2015.

[11] Syed Abdul Basit, and Manoj Kumar, "A Review of Routing Protocols for Underwater Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 12, December 2015.

[12] M. Ahmadia, and S. M. Jameii, "A Secure Routing Algorithm for Underwater Wireless Sensor Networks", IJE Transactions, Vol. 31, No. 10, October 2018.

[13] Mari Carmen Domingo, "Securing Underwater Wireless Communication Networks", IEEE Wireless Communications, February 2011.

[14] Rogaia Mhemed, William Phillips, Frank Comeau and Nauman Aslam, "Void Avoiding Opportunistic Routing Protocols for Underwater

Wireless Sensor Networks: A Survey", 6 December 2022.

[15] Syed Mohtashim Mian, and Dr. Rajeev Kumar, "Security Analysis and Issues in Underwater Wireless Sensor Auditory and Multipath Network", The International journal of analytical and experimental modal analysis, October-2019.

[16] Mohammad Alsulami, Rafaat Elfouly and Reda Ammar, "Underwater Wireless Sensor Networks: A Review", 2022.

[17] A.Rehash Rushmi Pavitra, L.Karthika, P.Uma Maheswari, S.Keerthana, and K.Rupiya, "A Survival Study on Flooding based Routing Protocols for Underwater Wireless Sensor Networks", Journal of University of Shanghai for Science and Technology, Volume 24, Issue 8, August - 2022.

[18] Guang Yang, Lie Dai, Guannan Si, Shuxin Wang, and Shouqiang Wang, "Challenges and Security Issues in Underwater Wireless Sensor Networks", International Conference on Identification, Information and Knowledge in the Internet of Things, 2018.

[19] Manal Al-Bzoor, Walaa Ayyad, and Ola Alta'ani, "A Survey on Efficient Routing Strategies for the Internet of Underwater Things (IoUT)", Journal of Electronics and Telecommunications, vol. 68, no. 4, 2022.