

**Secure and Lightweight Key Management
Framework for Underwater Wireless Sensor
Networks**



Sabir Shah
153-FBAS/PHDCS/F16

Supervisor

Dr. Asim Munir
Assistant Professor, DCS, IIU

Co-Supervisor

Dr. Abdul Waheed
Assistant Professor, DCS, Women University Swabi

Department of Computer Science
Faculty of Computing and Information Technology
International Islamic University, Islamabad, Pakistan
2024



^{VH}
JH-26912

PHD
105.824
SAS

Wireless sensor networks
ultrasound acoustics
Computer security
cryptography
key management (Computer security)

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD
FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE

Date: 05-07-2024

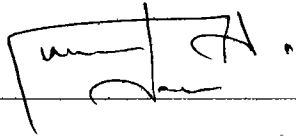
Final Approval

It is certified that we have read this thesis, entitled “**Secure and Lightweight Key Management Framework for Underwater Wireless Sensor Networks**” submitted by **Mr. Sabir Shah, Registration No. 153-FBAS/PHDCS/F16**. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for the award of the degree of PhD in Computer Science.

Committee


External Examiner:

Dr. Munam Ali Shah,
Assistant Professor
COMSATS University, Islamabad



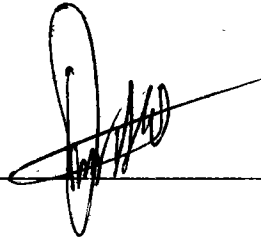
External Examiner:

Dr. Ata Ullah,
Assistant Professor
NUML University, Islamabad



Internal Examiner:

Dr. Qammar Abbas,
Assistant Professor
Department of Computer Science, FCIT, IIUI



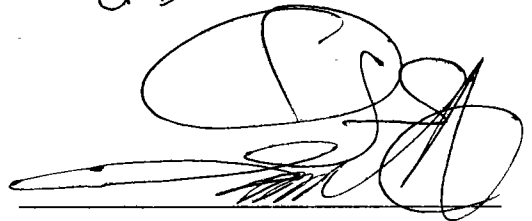
Supervisor:

Dr. Asim Munir,
Assistant Professor
Department of Computer Science, FCIT, IIUI



Co-Supervisor:

Dr. Abdul Waheed,
Assistant Professor
DCS, Women University, SWABI



*A dissertation submitted to the
Department of Computer Science
International Islamic University, Islamabad
as a partial fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy in Computer Science.*

Declaration

I, Sabir Shah, hereby declare that my Ph.D. thesis titled “*Secure and Lightweight Key Management Framework for Underwater Wireless Sensor Networks*,” is my work, neither as a whole nor as a part thereof has been copied out from any source except where due reference is made in the text. It is further declared that I have not previously submitted the work presented in the thesis report for partial or full credit for the award of degree at this or any other university.

Sabir Shah

153-FBAS/PHDCS/F16

Acknowledgments

I am deeply grateful to Almighty Allah for His favors and blessings, which encouraged me to work on writing this dissertation. I owe thanks to Allah SWT for giving me a life full of strength and inspiration to accomplish this task.

Moreover, I would like to express my gratitude to my supervisor, Dr. Asim Munir, who provided me with valuable advice and cooperation, which enabled me to carry out this entire work. It was an honor working under his supervision.

Furthermore, I also extend special thanks to Dr. Abdul Waheed, the co-supervisor. It has been a privilege to have his insight and academic support. I am humbly thankful for his availability, generosity, fruitful discussions, and remarks that helped me to improve the entire work.

Last but not least, I express my gratitude to all my family, teachers, and friends whose well wishes motivated me a lot in fulfilling this task.

Sabir Shah

153-FBAS/PHDCS/F16

Dedication

*To My
Parents Babba, Mama,
Brothers, Sisters, Wife, Kids
Teachers,
Colleagues
and
Friends*

Abstract

In the realm of Underwater Wireless Sensor Networks (UWSNs), the need for efficient and robust security measures is paramount due to the distinct challenges and limitations these networks face. The focus of this dissertation is on advancing the security boundaries of UWSNs by presenting a holistic framework for key management, along with a generalized signcryption scheme and an adaptive trust model. This research introduces a cost-efficient key management framework for UWSNs based on Elliptic Curve Cryptography (ECC) with lightweight implementation of pre-distributed keys, pairwise keys, group keys, and forward secure session keys. The proposed key management framework is compared with state-of-the-art KPIS, QKD, and LEAP in terms of key distribution time, memory usage, and energy consumption. The proposed framework consumed 7.5J energy with 40s time and 6KB memory. In terms of digital signature and encryption, the generalized signcryption scheme is tailored for UWSN's communication. Considering the dynamic environment, only encryption mode, only signature mode, and signcryption modes are evaluated for confidentiality, integrity, non-repudiation, and authentication. A generalized signcryption scheme is compared with existing schemes in terms of computation and communication overheads. The Signcryption and unsigncryption times are 8.9ms and 8.4ms respectively, the computation time is 17.3ms and the communication overhead is 46 bytes showing that the proposed scheme is feasible for UWSNs. Moving sensor nodes among different networks, the sink nodes calculate the trust values of sensor nodes and share for integrity. An adaptive trust model is formulated based on a modified decision tree to calculate trust. This model is designed specifically for underwater conditions, ensuring that sensor nodes operate within a trust-enhanced environment and effectively mitigating malicious nodes and potential threats. The proposed trust-enhanced model collects information from sensed data and calculates the trust score. Based on the modified decision tree, trusts were evaluated with 100 nodes having parameters (BR, ISR, ES, FS). Out of 100, 25 malicious nodes are included in a homogeneous network. 24 nodes are correctly identified and one false positive. 94 % accurately identified. The model accuracy is 94 % in heterogeneous, 92 % in high traffic network, and 96% in low traffic networks respectively. The proposed model is compared with state-of-the-art frameworks, accurately, with less false positive rate, minimum overhead, minimum power usage, and low response time.

Research Contribution

The following research papers related to this thesis are published/submitted in international conferences and journals during my Ph.D. research.

International Journal Publication:

1. **S. Sabir**, A. Munir, A. Waheed., " Enhancing Security and Efficiency in Underwater Wireless Sensor Networks: A Lightweight Key Management Framework," *Symmetry*, 2023.

[Published (IF: 2.833)]

2. **S. Sabir**, A. Munir, A. Waheed., "A novel lightweight generalized signcryption scheme for underwater wireless sensor networks"

[Submitted]

3. **S. Sabir**, A. Munir, A. Waheed., A Dynamic Trust Evaluation and Update Mechanism Based on Modified Decision Tree in Underwater Wireless Sensor Networks

[Submitted]

Table of Contents

Chapter 1	1
Introduction.....	1
1.1 Key Management Framework.....	2
1.2 Generalized Signcryption.....	3
1.3 Trust Management.....	4
1.4 Challenges and Requirements	4
1.5 Aim and Objectives.....	6
1.6 Scope of the Study.....	6
1.7 Research Contribution.....	7
1.8 Structure of the Thesis.....	7
Chapter 2	10
Literature Review	10
2.1 Existing Key Management Frameworks	10
2.2 Symmetric and Asymmetric Key Management in UWSNs.....	11
2.3 Challenges in UWSN Key Management.....	12
2.4 Basics of Signcryption	15
2.5 Signcryption in UWSNs.....	16
2.6 Existing Signcryption Schemes in UWSNs	17
2.7 Limitations of Current Approaches.....	20
2.8 Traditional Trust Evaluation Mechanisms in UWSNs.....	21
2.9 Decision Tree-Based Approaches in Other Networks	24
2.10 Identified Gaps in Existing Literature	24
2.11 Problem Statement	25
2.11.1 Problem Statement 1 (Key Management)	26
2.11.2 Problem Statement 2 (Signature and Encryption)	26
2.11.3 Problem Statement 3 (Node Mobility and Trust Management)	26
2.12 Research Questions	26
2.14 Chapter Summary.....	27
Chapter 3	28
UWSNs Methodology.....	28
3.1 Evaluation Parameters.....	29
3.1.1 Computation Cost.....	29
3.1.2 Communication Cost	30

3.1.3 Security Analysis in UWSNs Security	30
3.2 Preliminaries.....	31
3.3 Simulation and Performance Evaluation.....	34
Chapter 4	36
Key Management Framework	36
4.1 Key Generation Algorithm.....	36
4.2 Key Distribution Mechanisms.....	38
4.3 Key Revocation Mechanisms.....	40
4.4 Certificate Revocation List (CRL)	40
4.5 Authentication Mechanisms.....	40
4.5.1 Public Key Infrastructure (PKI)	41
4.5.2 Other Authentication Mechanisms	41
4.6 Lightweight Implementation	42
4.6.1 Pre-distributed Keys	43
4.6.2 Pairwise keys.....	44
4.6.3 Group keys.....	45
4.7 Performance Metrics	45
4.8 Chapter Summary.....	48
Chapter 5	49
Secure Generalized Signcryption Scheme	49
5.1 Secure Generalized Signcryption Scheme	49
5.2 Detailed Scheme Description.....	50
5.3 Security Analysis of Generalized Signcryption Scheme	51
5.3.1 Confidentiality	51
5.3.2 Authentication and Non-repudiation	52
5.3.3 Resistance to Man-in-the-Middle Attacks (MitM).....	52
5.4 Performance Evaluation	52
5.5 Efficiency Analysis	53
5.6 Comparison with Existing Schemes.....	54
5.7 Strengthen of the Proposed Scheme.....	58
5.8 Chapter Summary.....	62
Chapter 6	64
Dynamic Trust Evaluation	64
6.1 The Modified Decision Tree Algorithm.....	64
6.1.1 Basics of Decision Tree Algorithms.....	64

6.1.2 Modifications Tailored for UWSNs	65
6.2 Models of the proposed scheme	68
6.2.1 System Model	68
6.2.2 Network Model.....	70
6.2.3 Threat Model	71
6.3 Trust Evaluation Process	73
6.3.1 Data Acquisition and Preprocessing	73
6.3.2 Trust Score Computation.....	73
6.3.3 Dynamic Update Mechanism	75
6.4 Performance Evaluation	77
6.4.1 Experimental Setup.....	77
6.4.2 Results and Discussion	78
6.5 Chapter Summary.....	85
Chapter 7	86
Conclusion and Future Work	86
7.1 Conclusion.....	86
7.2 Future Direction	87
References	88

List of Tables

Table 2.1: Critical Evaluation of Existing Keys Management Techniques in UWSNs..... 14

Table 2.2: Comparison of Signcryption with Traditional Approaches 16

Table 2.3: Comparison of UWSNs with Terrestrial WSNs 16

Table 2.4: Critical Review of State-of-the-art Signcryption Schemes..... 19

Table 2.5: Comparison of Signcryption Schemes for UWSNs..... 20

Table 2.6: Limitations of Signcryption Schemes in UWSNs 21

Table 2.7: Comparison of Traditional Trust Evaluation Mechanisms in UWSNs..... 22

Table 2.8: Critical Review of Existing Trust Evaluation Models..... 23

Table 2.9: Comparison of Decision Tree-Based Approaches in Various Networks..... 24

Table 3.1: Notation and Description for Definitions 31

Table 3.2: Performance Metrics Parameters 35

Table 3.3: Simulation parameters used in the performance evaluation. 35

Table 4.1: Notation for Key Generation 37

Table 4.2: Point Addition and Multiplication 43

Table 4.3: Key Distribution Time Comparison for Different Key Distribution Mechanisms .46

Table 4.4: Memory usage Comparison for different Key Distribution Mechanisms..... 46

Table 4.5: Energy Consumption Comparison for Different Key Distribution Mechanisms ... 46

Table 4.6: Comparison with State of Art Techniques..... 47

Table 4.7: Comparison with state of art techniques..... 47

Table 5.1: Experimental Setup Specifications 53

Table 5.2: Computation Time (in milliseconds) for Different Schemes 53

Table 5.3: Communication Overhead (in bytes) for Different Schemes 54

Table 5.4: Energy Consumption (in Joules) for Different Schemes 54

Table 5.5: Computation Time (in milliseconds) for Different Schemes..... 55

Table 5.6: Communication Overhead (in bytes) for Different Schemes 56

Table 5.7: Energy Consumption (in millijoules) for Different Schemes 56

Table 5.8: Limitations of Proposed Scheme 60

Table 5.9: Countermeasures for Identified Limitations 60

Table 6.1: Key Components and Attributes of the Network Model 68

Table 6.2: Capabilities of Sensor Node 70

Table 6.3: Data Acquisition and Preprocessing Steps 73

Table 6. 4: Parameter and Description..... 75

Table 6.5: Trusted and Malicious Nodes 78

Table 6.6: Trust Evaluation Accuracy in Different Scenarios 79

Table 6.7: False Negative Rates in Different Scenarios 80

Table 6.8: Comparative Analysis of Trust Evaluation Mechanisms..... 81

Table 6.9: Network Performance Metrics Overview 83

List of Figures

Figure 1.1: Overview of Underwater Wireless Sensor Network (UWSN).....	1
Figure 1.2: Chapter wise Structure of Thesis.....	9
Figure 3.1: Methodology of UWSNs.....	29
Figure 4.1: Proposed Key management model for UWSNs.....	36
Figure 4.2: Network Model of Keys Management Framework.....	41
Figure 4.3: Communication of Nodes in Proposed Lightweight Approach.....	42
Figure 4.4: Performance evaluation for pre-distributed keys mechanism.....	43
Figure 4.5: Performance evaluation for pairwise keys mechanism.....	44
Figure 4.6: Performance evaluation for group keys mechanism.....	45
Figure 5.1: Signcryption and Unsigncryption Communication Model.....	50
Figure 5.2: Computation Time Across Different Schemes.....	55
Figure 5.3: Communication overhead across various Schemes.....	56
Figure 5.4: Energy consumption across various Signcryption Schemes.....	57
Figure 5.5: Performance of the Proposed Scheme across different Network Sizes.....	59
Figure 5.6: Integration of the Proposed Scheme with various UWSN architectures.....	59
Figure 5.7: Node Capacity and Computational Load.....	61
Figure 5.8: Environmental Adaptation Chart.....	61
Figure 5.9: Implementation Ease Matrix.....	62
Figure 6.1: System model of UWSNs.....	69
Figure 6.2: Network Model of UWSNs.....	71
Figure 6.3: Threat Model.....	72
Figure 6.4: Trust Score.....	79
Figure 6.5: Line Graph of Accuracy Trend Over Time.....	81
Figure 6.6: Accuracy Comparison Various Methods.....	82
Figure 6.7: Response Time Trend.....	83
Figure 6.8: Throughput Comparison of Existing Methods.....	84
Figure 6.9: Latency Trends.....	84

List of Acronyms

BDHP	Bi-Linear Diffie-Hellman Problem
BP	Bilinear Pair
BR	Behavioral Reliability
CA	Certificate Authority
CDHP	Computational Diffie-Hellman Problem
CH	Cluster Head
CLC	Certificateless Cryptosystem
DBDHP	Decisional Bi-Linear Diffie-Hellman Problem
DBTM	Distributed Bayesian Trust Model
DH	Diffie-Hellman
DH	Diffie-Hellman
DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ES	Energy Sustainability
FLTM	Fuzzy Logic-based Trust Model
FS	Feedback Score
GC	Galois Counter
GDHP	Gap Diffie-Hellman Problem
HECC	Hyper Elliptic Curve Cryptography
IBC	Identity Base Cryptosystem
ISR	Interaction Success Rate
MMR	Multi-Metric-Reputation
PKC	Public Key Cryptosystem
PKI	Public Key Infrastructure
PUP	Physical Unclonable Function
RSA	Rivest-Shamir-Adleman
RSS	Receiver Signal Strength
SGSS	Secure Generalized Signcryption Scheme
TS	Trust Score
UWSNs	Underwater Wireless Sensor Networks
VPS	Virtual Phase Shift
WSN	Wireless Sensor Network

Chapter 1

Introduction

UWSNs have developed as a potentially useful technology for a variety of applications that take place underwater, including oceanographic monitoring, environmental monitoring, and underwater surveillance [1]. UWSNs consist of many sensor nodes that are deployed in the underwater environment to gather data and transmit it to the sink node as shown in Figure 1.1. However, UWSNs face several challenges such as the harsh underwater environment, limited communication range, and low data rates [2]. These networks play a pivotal role in efficiently gathering and transmitting critical data from underwater environments to the surface for further analysis and informed decision-making[3]. Nevertheless, the unique underwater conditions present formidable challenges to the functionality and security of UWSNs[4]. Challenges such as restricted bandwidth, substantial propagation delays, and susceptibility to various malicious attacks underscore the necessity for robust security measures in these networks[5]. Consequently, developing innovative and effective security solutions is of paramount importance to ensure the integrity, confidentiality, and availability of the transmitted data in UWSNs [6]. One of the critical challenges is to develop a secure

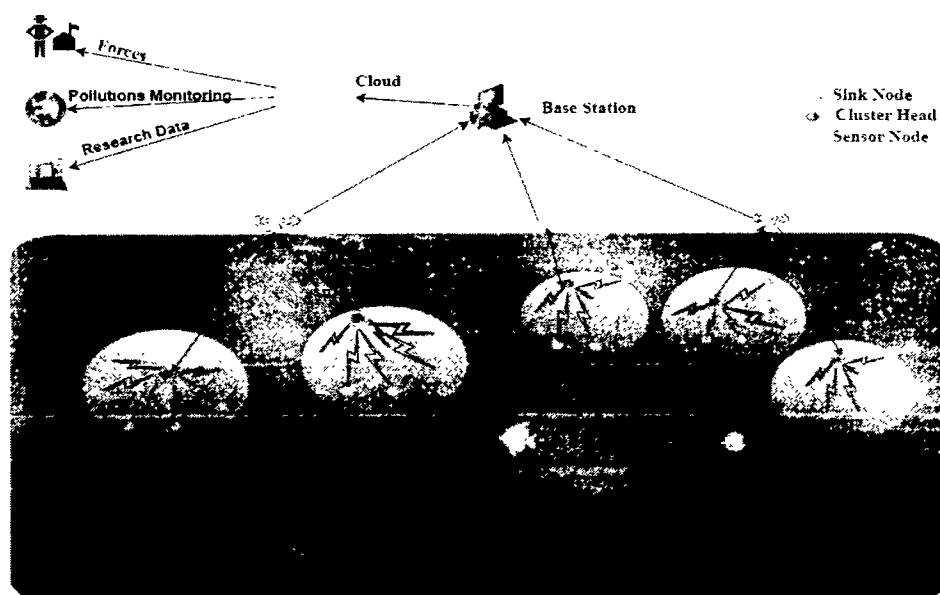


Figure 1.1: Overview of Underwater Wireless Sensor Network (UWSN)

and lightweight key management framework that ensures the security of the network and prevents unauthorized access [7, 8]. Key management is an essential component of any secure communication system, and it plays a critical role in UWSNs. Key management involves generating, distributing, and revoking cryptographic keys to encrypt and decrypt data. A secure key management system guarantees the confidentiality, integrity, and availability of the data transmitted over the network and ensures that only authorized nodes may access it [9]. Key management is a fundamental component of any secure communication system, and it plays a critical role in UWSNs [10]. A secure key management system guarantees that only authorized nodes can access the network and that data communicated over the network is confidential. Several key management frameworks have been proposed for UWSNs, but most of them have limitations such as high processing overhead, limited scalability, and vulnerability to attacks [11]. Therefore, there is a need for a secure and lightweight key management framework that can address the challenges of UWSNs and ensure the security of the network.

1.1 Key Management Framework

A secure and lightweight key management framework for UWSNs that combines symmetric and asymmetric encryption, uses lightweight cryptography algorithms and ensures scalability [12]. Hybrid key management frameworks provide better security in terms of symmetric and public key approaches [13]. The proposed framework includes a robust key generation algorithm, fault-tolerant key distribution mechanisms, a key revocation mechanism, an authentication mechanism, and a lightweight implementation. There are three distinct methods for handling keys in UWSNs; they are centralized, hierarchical, and distributed [14]. A network that uses centralized key management has one governing body that generates and distributes keys to all other nodes. Hierarchical key management divides the network into clusters, and a cluster head is responsible for generating and distributing keys to nodes within the cluster. Distributed key management involves nodes generating and distributing their keys.

UWSNs are a less explored area and get more attention from research communities due to their vast range of applications. In such a resource-constrained environment, sensors are vulnerable to all known attacks. Recognizing the importance of addressing the security concerns, the proposed lightweight and secure Elliptic curve cryptography

(ECC) based framework is efficient and computationally feasible as compared to the existing frameworks. Secure and lightweight keys play a vital role in terms of encryption and digital signature. Using the above lightweight generated keys for encryption and signature creates overhead in such a resource-constrained environment and it became two logical steps.

1.2 Generalized Signcryption

Traditional encryption and signature protocols might be insufficient given the distinct constraints of underwater communication. Signcryption, a fusion of the encryption and signature processes, has been highlighted as an effective strategy in various arenas because of its inherent efficiency [15]. The pressing requirement now is to devise a signcryption technique that's not only specific to the challenges of UWSNs but is also resource efficient. Such an approach would address the dual objectives of ensuring data confidentiality and optimizing energy use in the sensor nodes, a crucial aspect given the limited power resources in these networks [16]. In the expanding landscape of UWSNs, ensuring both effective communication and security remains a dual challenge. While previous studies have broached the subject from varying angles, this research introduces innovations that distinctively bridge the gaps observed in prior endeavors.

Public Key Infrastructure (PKI), IBC (identity-based cryptosystem), and certificateless cryptosystem (CLC) [17]. The PKI-based approach is unstable in a resource-constrained environment due to certificate management. IBC-based techniques are more vulnerable to third-party attacks like key escrow issues. Private key generation (PKG) has all private key information. PKG suffers from a private key escrow problem. The CLC solves the issue of key escrow by using the partial key and secret values having key distribution issues.

Signcryption is another public key scheme proposed by Zheng [18] for the first time in a single logical step to solve computation and communication overhead in such a resource-constrained environment. Traditional approaches “signature-then-encryption” are computationally expensive due to two logical steps. A single logical step signcryption reduces up to 50% computation cost and up to 80% communication cost [19]. Using diverse signcryption in Bilinear pairing-based cryptographic scheme results in complexity with some irregular security parameters which diversify the advantages from smaller key size, yet in Diffie-Hellman heterogeneous signcryption, the overall

communication overhead was minimized. By solving the traditional sign-then-encrypt issue through signcryption. Node mobility in UWSNs is another key issue that the research community addressed over the last few years. To solve mobility issues among clusters and sink node regions, trust management is another unavoidable approach in UWSNs.

1.3 Trust Management

Trust plays a pivotal role in the effective functioning of (UWSNs). Given the remote and often inaccessible nature of underwater deployments, ensuring the reliability and authenticity of data becomes paramount. Trust mechanisms help in discerning the credibility of sensor nodes and the data they transmit. In applications like marine ecosystem monitoring or underwater seismic detection, the accuracy of data is crucial. A compromised or malfunctioning node can transmit erroneous data, leading to incorrect analyses or conclusions [20]. UWSNs are vulnerable to various security threats, including eavesdropping, man-in-the-middle attacks, and node impersonation. Trust mechanisms can identify and isolate malicious nodes, ensuring the overall security of the network [21]. In the resource-constrained underwater environment, where energy is at a premium, trust mechanisms ensure that communication resources are not wasted on unreliable or malicious nodes. This prolongs the network's operational lifespan [22]. In the dynamic underwater environment, nodes may frequently lose connectivity due to water currents or marine life interference. Trust mechanisms can aid in making informed decisions about routing data through the most reliable nodes, ensuring data reaches its destination [23].

1.4 Challenges and Requirements

Underwater wireless sensor networks (UWSNs) have several challenges in terms of security due to harsh underwater environments and resource constraints on sensor nodes. Secure Communication among nodes is a significant concern, as underwater communication channels are vulnerable to jamming, eavesdropping, and unauthorized access to nodes and channels. Developing secure communication protocols and encryption mechanisms that can withstand these threats is an ongoing challenge. The following are key challenges of UWSNs.

- **Communication Security**

In UWSNs, securing communication is challenging due to the unique underwater environment. Factors like limited bandwidth, high latency, and the use of acoustic channels (which have different properties compared to radio frequencies) complicate the implementation of standard security measures.

- **Key management**

Effective key management is crucial for secure communication. In UWSNs, the distribution and management of encryption keys must cope with the network's dynamic nature and the limited computational capabilities of underwater sensors.

- **Nodes Authentication**

Ensuring that each node in a UWSN is legitimate and has not been tampered with is a significant challenge. Robust authentication mechanisms are required to prevent unauthorized access and data manipulation.

- **Nodes compromising and physical attacks.**

Due to their often remote and inaccessible locations, UWSN nodes are vulnerable to physical attacks and tampering. This could lead to compromised data integrity and network functionality.

- **Storage of keys and data security**

Storing encryption keys securely in sensor nodes is a challenge due to their limited memory and computational power. Additionally, ensuring the security of the data stored in these nodes is paramount, as it often includes sensitive information.

- **Trust Management**

Establishing and managing trust in UWSNs involves ensuring that the networked nodes and the data they transmit are reliable. This is complicated by the harsh underwater environment and the potential for nodes to be compromised.

- **Secure Positioning and Localization**

Accurate and secure positioning is vital for many UWSN applications. However, ensuring that the location data of nodes is not tampered with or spoofed is a complex task, especially given the unique propagation delays and movement patterns in underwater environments.

1.5 Aim and Objectives

The research work aims to present a secure, lightweight key management framework, Generalized signcryption, and trust management mechanism for UWSNs.

The objective of the research work is to design and secure schemes for Underwater communicational setup. The main objectives of the study are:

1. Design and implement a lightweight key management framework that encompasses key generation, distribution, and revocation mechanisms to minimize computational and communication overheads to enhance the efficiency and security of UWSNs.
2. To develop a secure generalized single logical step signcryption scheme to integrate signature and encryption functionalities and minimize computational and communication overheads in standard/Oracle Models.
3. To develop a trust evaluation mechanism that considers diverse node attributes and addresses mobility issues in dynamic and resource-constrained UWSNs.
4. The developed methods should secure against all known attacks with forward security and public verifiable in UWSNs.

Evaluation of the security and cost of state-of-the-art schemes/frameworks using Game theory /mathematical/simulation tools.

1.6 Scope of the Study

The scope of the Secure and Lightweight key management framework in terms of UWSNs is broad. The findings and outcomes of this study have many application domains, like underwater environment monitoring, surveillance systems, submarine, and tsunami detection. This research focuses on the applications domain using resource-constrained underwater wireless sensor networks that are vulnerable to known attacks on integrity, confidentiality, authentication, and non-repudiation. The key management framework solved the key generation, key distribution, and key revocation issues while the signcryption is a computationally inexpensive approach performed in a single logical step.

1.7 Research Contribution

The following novel contribution has been made in the field of UWSNs Security.

1. Lightweight key management framework comprises key generation, distribution, and revocation.
2. Computationally feasible generalized signcryption scheme for UWSNs.
3. Identification of trusted nodes considered the diverse attributes of resource constraint nodes in dynamic environment UWSNs.
4. Forward secure and public verifiable framework resist against all known attacks.

1.8 Structure of the Thesis

The structure of the thesis is organized as follows and summarized in Figure 1.2:

Chapter 1: Introduction to Underwater Wireless Sensor Networks (UWSNs), Applications, Motivation, key challenges, and objectives of the research.

Chapter 2: In this chapter critically reviewed the key management, Signcryption, and trust management schemes/protocols/models.

Chapter 3: This chapter diagrammatically represents the thesis methodology, and evaluation parameters like communication cost, computation cost along with security analysis. The preliminaries of keys management, signcryption, and trust management are also discussed in this chapter. Furthermore, the simulation and performance evaluation with experimental setup are briefly discussed.

Chapter 4. This chapter consists of a key management framework. Public, private, and session key generation, distribution, and revocation in the PKI domain is discussed. Further results of pre-distribution, pairwise keys, and group key distribution methods are evaluated in terms of energy consumption, computation time, and memory usage.

Chapter 5: Secure generalized signcryption scheme for UWSNs is presented in this chapter. Security analysis like confidentiality, integrity, non-repudiation, and forward secrecy are examined. Performance evaluation and compared with existing approaches are evaluated in terms of a single logical step to combine both digital signature and secure communication.

Chapter 6: Dynamic trust evaluation to solve the node mobility issue among sink nodes domain/network is discussed. Real-time sensor node parameters are considered for trust values calculation with the system model, network model, and threat models. Lastly, trust evaluation and performance evaluation are examined and compared.

Chapter 7: Conclusion and future work of the thesis are presented in this chapter.

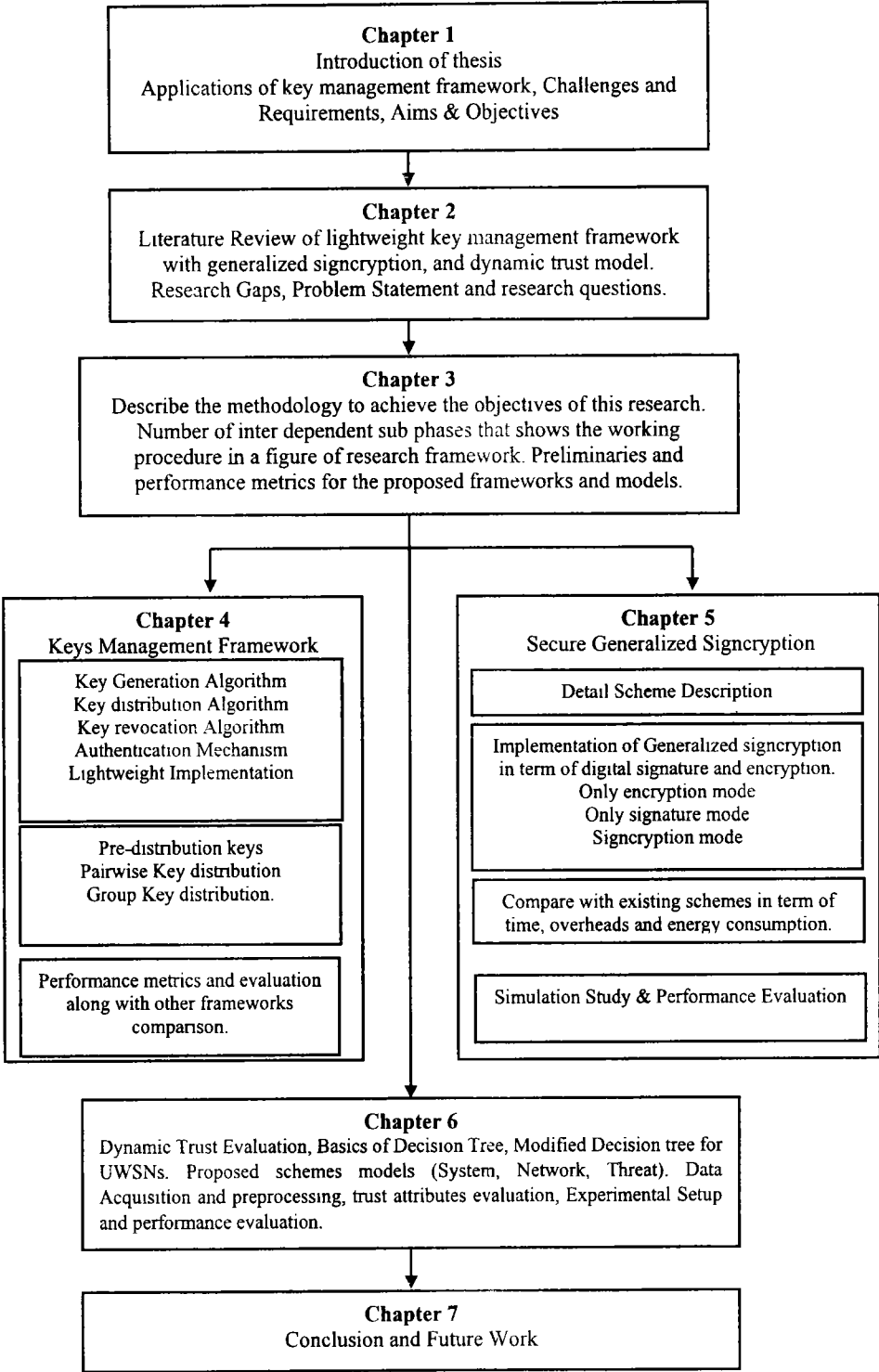


Figure 1.2: Chapter wise Structure of Thesis

Chapter 2

Literature Review

This chapter presents a comprehensive literature review that critically evaluates the existing key management frameworks and their applicability to UWSNs. Private, Public, and Session key management is the fundamental aspect of node authentication and secure communication in such a challenging environment. Various cryptographic schemes, approaches, frameworks, and protocols, distinguishing between symmetric and asymmetric key management, and exploring their respective strengths and weaknesses are discussed. The dynamic environmental conditions, limited node resources, and susceptibility to security breaches also examined different approaches of signcryption, trust evaluation, and decision-making processes for node mobility. The chapter identifies gaps in current research and underscores the necessity for innovative frameworks that cater to the peculiarities of UWSNs. The critical evaluation of the existing key management, generalized signcryption, and trust management state-of-the-art approaches helped in finding and highlighting the latest advancements and persistent issues in the field.

2.1 Existing Key Management Frameworks

LEAP (Lightweight Encryption and Authentication Protocol) is a widely used key management framework that employs a public-key infrastructure (PKI) to generate, distribute, and revoke cryptographic keys. The LEAP protocol provides secure communication, but it has a high computational overhead for encryption and decryption, making it unsuitable for resource-constrained underwater sensor nodes [13]. Lu et al. [24] present LEAP-based cryptographic framework for CAN (Controlled Area Network). Stream cipher for message encryption and key management mechanisms are used to protect the network from external attacks. The proposed framework solved the integrity and confidentiality problems but due stream cipher method the synchronization, high data rate, and key distribution management are still addressable.

Another key management framework is the pairwise key pre-distribution scheme (PKPS) which uses a pre-distribution of symmetric keys to ensure secure communication. PKPS distributes keys before deployment, and these keys are stored in the memory of the sensor nodes. However, PKPS suffers from scalability issues and requires many keys to be preloaded into the sensor nodes, making it unsuitable for large-scale UWSNs [25]. Pairwise key pre-distribution creates problems in random deployments of sensors because of not knowing the locations in advance. The resiliency of node capture attacks and fast connectivity of sensor nodes, the authors presented a random small pool of key chains in the article [26].

Several key management frameworks have been proposed in the literature, such as HEED (Hybrid Energy-Efficient Distributed clustering), MMS (Multimodal Scheme), and QKD (Quantum Key Distribution). QKD-based approaches are proposed for secure communication and according to the authors resist all known eavesdropping attacks. In terms of UWSNs quantum based key distribution approaches can create complexities, vulnerabilities to noise interfaces and key management issues [27]. These frameworks use different approaches to ensure secure communication in UWSNs, such as clustering, multimodal sensing, and quantum cryptography. However, these frameworks have their limitations such as high processing overhead, limited scalability, and vulnerability to attacks [28]. Therefore, there is a need for a secure and lightweight key management framework that can overcome the limitations of existing frameworks and ensure the security of the network.

2.2 Symmetric and Asymmetric Key Management in UWSNs

Key management is a critical component of security in UWSNs, ensuring secure communication between sensor nodes. In UWSNs, key management frameworks are particularly divided into two categories. symmetric key and asymmetric key. Symmetric key management schemes are simple and efficient, but they are vulnerable to various attacks such as node capture and replay attacks. Asymmetric key management schemes provide a higher level of security but require a higher computational overhead for encryption and decryption, making them unsuitable for resource-constrained underwater sensor nodes [14]. Numerous key management frameworks have been proposed in the literature to address the challenges of UWSNs.

One of the most used frameworks is the Public Key Infrastructure (PKI) which uses an asymmetric key scheme to generate, distribute, and revoke cryptographic keys. However, PKI has a high computational overhead for encryption and decryption, making it unsuitable for resource-constrained underwater sensor nodes [29].

ECC-based asymmetric key management scheme used in various key management frameworks for wireless sensor networks. ECC provides a high level of security and is energy efficient. However, the existing state-of-the-art approaches are vulnerable to node capture attacks, where an attacker captures a node and retrieves its cryptographic key, making it unsuitable for UWSNs [30, 31]. Therefore, there is a need for a secure and lightweight key management framework that can overcome the limitations of existing frameworks and ensure the security of the network.

2.3 Challenges in UWSN Key Management

Key management in UWSNs faces several challenges due to the harsh underwater environment. One of the main challenges is the dynamic and unpredictable nature of the underwater environment. The changes in water currents, temperature, and salinity levels can affect the communication channel's performance and lead to issues such as packet loss, signal attenuation, and interference, which can cause the loss of cryptographic keys [32]. Another significant challenge is the limited resources of the underwater sensor nodes, having less energy and limited computation power. These limitations make it challenging to use computationally expensive key management schemes such as asymmetric key encryption algorithms, which require more processing power and memory [33]. UWSNs are vulnerable to various security attacks, such as node capture, sinkhole, and wormhole attacks, which can compromise the network's security. For instance, node capture attacks can lead to the theft of cryptographic keys, while sinkhole attacks can redirect the communication flow to an attacker's node, making it difficult to establish a secure communication channel [34]. Mezrag et al. [35] proposed an identity-based cryptographic scheme for secure communication with ECC based key distribution model to resist all known common attacks. The RC5-based cognitive key management scheme is used for key management. Easy implementable. F. Khan et al. [36] established CH based key management is used to cause additional overhead. The maximum key size is 2048 bits for secure encryption which is infeasible

UWSNs. Key issues to the identity-based cryptographic schemes are trust among sensor nodes, scalability, and key escrow. Muhajjar et al [37] proposed PKMS for solving the complexities of CBC-RC5 Using the PNGR and matrix multiplication. Matrix multiplication creates additional overhead. Yang et al [38] presented a signature-based scheme for message verification in UWSNs. Traditional schemes are computationally not feasible for resource-constrained environments. ECC-based lightweight schemes reduce computation costs and resist attacks like node compromise and message medication. Furthermore, the scalability of key distribution is another significant challenge in UWSN key management. Large-scale UWSNs with thousands of sensor nodes make it challenging to distribute unique keys to each node. Therefore, efficient key distribution and management schemes are necessary to reduce the overhead of key distribution and minimize the risk of key compromise [39]. A prominent approach, highlighted by [40], combines the strengths of symmetric and asymmetric encryption, utilizing dynamic key generation mechanisms. This technique offers robust defenses against various attacks, especially brute force attempts, and boasts superior execution time. However, its complexity and potential overhead, particularly when multiple users are involved, present challenges. Mobile networks, particularly Mobile Ad Hoc Networks (MANETs), present their own unique set of challenges. In this realm, [41] proposes a tailored key management solution that merges cryptographic strengths with node behavior analysis. While promising, concerns about overhead, scalability, and reliance on node behavior analysis underscore potential challenges in its widespread adoption. The domain of quantum technologies offers a plethora of opportunities and challenges. The article by [42] delves deep into this, introducing a comprehensive assessment framework for quantum networks. The emphasis on higher security against eavesdropping and other traditional cyber threats is noteworthy. However, the nascent nature of quantum technologies and concerns about integration with classical networks make its widespread deployment a topic of debate. Blockchain technology's integration into key management has garnered significant attention. The study by [43] leverages blockchain's decentralized nature for healthcare applications. While promising, concerns like scalability and latency associated with blockchain might pose practical challenges. Another mechanism discussed by Gowda et al. [44] tailors a blockchain approach for fog computing. The promise of enhanced security in fog environments is evident, but the inherent challenges of blockchain, like performance overhead, cannot be ignored. The potential of Elliptic Curve Cryptography (ECC) for remote user

authentication is explored by Chatterjee et al. [45] and the ECC-based method, being both lightweight and secure, offers an efficient mutual authentication mechanism. Yet, the complexities and potential limitations of ECC, coupled with dependencies on secure channels, present challenges.

To address these challenges, a secure and lightweight key management framework is required for UWSNs that can efficiently distribute and manage cryptographic keys, provide a high level of security, and overcome the limitations of existing key management schemes briefly described in Table 2.1.

Table 2.1: Critical Evaluation of Existing Keys Management Techniques in UWSNs

Ref.	Study Focus	Key Findings
[24] (2022)	LEA protocol for Controlled Area Network	Solve integrity and confidentiality issues. Due to the stream cipher method, the synchronization, high error rate, and key management issues are still addressable.
[26] (2022)	Pairwise key distribution in Wireless Sensor Network	Random pre-distribution with a small key chain solves the location issue of sensor nodes. Scalability, flexibility, and key management are the main issues
[29] (2020)	Secure communication of UWSN	Symmetric key algorithms are used for secure communication and authentication
[35] (2022)	Identity-based Cryptographic scheme for WSNs	Lightweight and easily implementable The main issues are trust, scalability, and key escrow
[36] 2019	CKMS	The RC5-based cognitive key management scheme is used for key management. Easy implementable. CH-based key management is used to cause additional overhead. The maximum key size is 2048 bits for secure encryption which is infeasible UWSNs.
[37] (2023)	Perfect Security Key Management (PSKM)	Solve CBC and RC5 complexities for key management using PNGR and matrix multiplication. Multiplying the Key matrix with the public matrix creates additional overhead in such a resource-constrained environment.
[38] (2018)	Signature scheme for UWSNs	Resist against node compromise and message modification attacks. Due to the fuzzy-based EDAS technique, the issues are adaptability, scalability, and additional computation overhead.
[40] (2022)	Cryptographic algorithm using dynamic key generation for cloud storage	Efficient against brute force attacks; Superior execution time. Complex implementation; Concerns about user credential security.
[41] (2022)	Key management in Mobile Ad Hoc Networks (MANETs)	Effective use of cryptographic techniques and node behavior analysis Scalability concerns; Overhead due to behavioral analysis.

Ref.	Study Focus	Key Findings
[42] (2022)	Quantum networks' security assessment and key management	High security against traditional cyber threats Challenges in integrating with classical networks, Nascent technology.
[43] (2023)	Blockchain-based key management for healthcare	Enhanced security tailored for healthcare, Decentralized approach. Scalability concerns; Potential latency issues.
[44] (2023)	Key management for fog computing using blockchain	Improved security for fog environments; Addressed fog computing challenges. Performance overhead; Complexity of blockchain integration.
[45] (2022)	Remote user authentication using Elliptic Curve Cryptography (ECC)	Lightweight and efficient for remote scenarios. Inherent complexities of ECC; Potential implementation errors with ECC.

2.4 Basics of Signcryption

The concept of signcryption was first introduced by Zheng in 1997 to achieve the combined functionality of digital signatures and encryption at a lower computational cost than executing both processes separately [46]. Since its inception, the methodology has been adapted and refined to cater to diverse communication environments.

Signcryption operates in three primary phases: key generation, signcryption, and unsigncryption [47]. The key generation phase produces public-private key pairs for users. During signcryption, a sender uses their private key and the recipient's public key to produce a signcrypted message. The unsigncryption phase allows the recipient to decrypt the received message and verify its authenticity simultaneously [48]. The primary motivation behind signcryption was to provide an efficient means of ensuring data integrity and confidentiality. Studies have shown that signcryption can be substantially faster than the combined process of signature followed by encryption [49]. By integrating signature and encryption, signcryption ensures that messages are not only confidential but also authenticated, offering protection against both external eavesdropping and tampering [50]. Table 2.2 present the comparison of Comparison of Signcryption with various Traditional Approaches.

Table 2.2: Comparison of Signcryption with Traditional Approaches

Feature	Signcryption	Signature + Encryption
Computational Complexity	Moderate	High
Data Integrity	✓	✓
Data Confidentiality	✓	✓
Combined Operation Cost	Low	Moderate to High
Adaptability to UWSNs	Under Research	Moderate

While signcryption offers numerous advantages, it's not devoid of challenges. Ensuring universality (adaptability across different platforms) and addressing potential vulnerabilities specific to signcryption methods are areas of ongoing research [51].

2.5 Signcryption in UWSNs

UWSNs play a pivotal role in exploring and monitoring the aquatic environment. Comprising sensor nodes and vehicles, these networks relay and process data across vast underwater expanses, enabling myriad applications, from environmental monitoring to strategic defense operations. Sensor nodes in UWSNs are typically deployed across a specified region, either by dropping them from the air or by submersible vehicles. Once active, these nodes gather data and communicate with each other, or to a surface station, primarily through acoustic communication channels given the inefficacy of radio waves underwater [52]. Unlike terrestrial networks, UWSNs largely rely on acoustic channels due to the rapid attenuation of radio and optical signals in water. Ocean currents can induce sensor node mobility, presenting challenges in consistent data collection and transmission [53]. Acoustic signals travel slower than electromagnetic signals, leading to higher propagation delays. Table 2.3 show Comparison of UWSNs.

Table 2.3: Comparison of UWSNs with Terrestrial WSNs

Feature	UWSNs	Terrestrial WSNs
Communication Medium	Acoustic channels	Radio frequencies
Node Mobility	Influenced by water currents	Typically, static
Propagation Speed	Approx. 1500 m/s	299,792,458 m/s (speed of light)
Energy Constraints	High (limited battery)	Moderate
Data Transmission Rate	Low to moderate	Moderate to high

Acoustic channels offer limited bandwidth, restricting data transfer rates [54]. Due to the remoteness of deployment locations and challenges in recharging, energy efficiency becomes paramount in UWSN design. Given their deployment in potentially unmonitored environments, UWSNs are susceptible to security breaches, necessitating robust cryptographic solutions [55].

2.6 Existing Signcryption Schemes in UWSNs

The unique environment of underwater wireless sensor networks (UWSNs) imposes several challenges, including high propagation delays, limited bandwidth, and energy constraints. Secure communication in this context is crucial, given the sensitivity of data and potential adversaries. Thus, signcryption has been viewed as a viable solution, providing both authentication and encryption in a single step. Over the years, various signcryption schemes have been proposed for UWSNs, addressing its unique challenges.

Signcryption in UWSNs is not just a direct application of traditional schemes. The inefficiencies of conventional algorithms, when used in underwater conditions, prompted the development of bespoke schemes optimized for the acoustic communication medium [56]. Shehzad Ashraf et al. [57] introduced an Elliptic Curve Cryptography (ECC) based scheme. ECC offers smaller key sizes than traditional methods, making it attractive for UWSNs. This scheme optimized computational costs while maintaining robust security. Xinying *et al.* [58] proposed an identity-based scheme that eliminates the need for certificates, thus reducing transmission overhead. This IBS technique offered efficiency and scalability, making it suitable for larger UWSN deployments.

The EMV-CLSC signcryption technique, as suggested by S. Alagarsamy and S. Rajagopalan [59], offers enhanced computational efficiency by reducing memory consumption during multiple data processing, although it struggles with the key escrow problem. A certificateless broadcast signcryption scheme, detailed mentioned by C. Zhou [60], successfully fulfills the requirements of multi-receiver signcryption in broadcast scenarios but faces challenges in preserving the privacy of the receiver's identity. In the domain of IoT, J. Qiu et al. [61] describe a certificateless broadcast signature and encryption method that improves applicability in IoT by outsourcing

signature verification, thereby reducing computational overhead. However, it does not include a receiver authorization set in the ciphertext, leading to challenges in accurately identifying the user-specific ciphertext. The approach of connecting edge nodes with IoT devices presented by X. Yu et al. [62], focuses on processing and analyzing massive IoT data before it is returned to the terminal device. The certificateless signature algorithm for underwater wireless media transmission, presented in G. Manikandan and U. Sakthi [63] scheme that effectively counters network layer attacks in wireless networks and distributes keys to sensor nodes. Nevertheless, it does not ensure data safety in underwater sensor networks due to the absence of a secure channel.

An identity-based hierarchical broadcast signcryption scheme, as proposed by C. Yuan et al. [64], proves to be effective for low-scale sensor networks but does not offer detailed security proof in the standard model. The identity-based signature scheme presented by Z. Zhou et al. [65] is publicly verifiable and encrypts messages solely with the sender's private key, allowing decryption with the public key of the sender. The encoding methodology using CNN for Laguerre Gaussian modes in turbulent channels is described in the A. Trichili et al. [66], leverages transfer learning for improved efficiency, applying pre-trained neural network knowledge. Yet, it does not address security implications adequately. The use of cable-connected sensor networks for underwater communication, mentioned by C.-C. Kao et al. [67], is widespread due to its ease of use but incurs high deployment costs. An energy-efficient encryption algorithm for underwater use, discussed in S. Goyal et al. [68], outperforms previous solutions in terms of energy efficiency. However, its 64-bit block size raises concerns about its applicability in standardized environments. The LP framework for energy overhead and route diversity, introduced in the D. Incebacak et al. [69], models energy consumption and focuses on security against node capture and eavesdropping attacks. Energy Level Based Hybrid Transmission (ELT), as proposed by J. Cao et al. [70], balances load by utilizing single-hop or multi-hop paths depending on the remaining energy of nodes, thus enhancing network lifetime. Energy efficient and secure data transmission method using chaotic compressive sensing (CCS) is described in W. C. Xinbin's [71] model. This method reduces transmission volumes through compressive sensing and enhances security with CCS-based encryption. Summarized critical review discussed in Table 2.4.

Table 2.4: Critical Review of State-of-the-art Signcryption Schemes

Ref.	Techniques/Approaches	Strengths	Weaknesses
[59] (2017)	EMV-CLSC signcryption technique	Improves computational efficiency by reducing memory consumption in multiple data processing.	The technique still suffered from key escrow problem
[60] (2019)	Certificateless broadcast signcryption scheme	Satisfies multi-receiver signcryption in a broadcast scenario. Cannot guarantee privacy preservation of receiver's identity; easy to reveal the receiver's identity	
[61] (2019)	Certificateless broadcast signature and encryption (IoT)	Improved applicability in IoT; outsourced signature verification to reduce computational overhead. Lacks receiver authorization set in the ciphertext; cannot accurately locate the ciphertext corresponding to the user	
[62] (2022)	Connectivity between edge nodes and IoT devices	Processes and analyses massive IoT data, returning it to the terminal device	
[63] (2018)	Certificateless signature algorithm for underwater wireless media transmission	Resists network layer attacks in wireless networks; distributes keys to sensor nodes. Does not provide a secure channel for data safety in underwater sensor networks	
[64] (2017)	Identity-based hierarchical broadcast signcryption scheme	The scheme is feasible for low-scale sensor networks. Does not provide detailed security proof in terms of a standard model.	
[65] (2022)	Identity-based signature scheme	The proposed scheme is publicly verifiable, the message is only encrypted with the private key of the sender, and Trent can decrypt the message with knowing the public key of the sender.	
[66] (2020)	Encoding methodology using CNN for Laguerre Gaussian modes in turbulent channels	Utilizes transfer learning for efficiency, pre-trained neural network knowledge application. Lack of security implications information	
[67] (2017)	Cable-connected sensor networks for underwater communication	Widely used due to ease of use. High deployment costs	
[68] (2022)	Energy-efficient encryption algorithm for UW	More energy-efficient than previous solutions. A block size of 64 bits poses questions of applicability in a standardized environment	
[69] (2015)	LP framework for energy overhead and route diversity	Models' energy consumption and security, focusing on security against node capture and eavesdropping attacks	
[70] (2013)	Energy Level Based Hybrid Transmission (ELT)	Balances load by using single-hop/multi-hop paths based on the remaining energy of nodes maintains better network lifetime	
[71] (2018)	Energy-efficient and secure data transmission using CCS	Reduces transmission amount using compressive sensing and improves security with CCS-based encryption	

Given the advancements in quantum computing, Patwary et al. [72] developed a signcryption scheme resistant to quantum attacks. This approach combined hash-based structures and lattice-based cryptography, ensuring future-proof security for UWSNs as shown in Table 2.5.

Table 2.5: Comparison of Signcryption Schemes for UWSNs

Scheme	Key Features	Strengths	Limitations
ECC-based Signcryption	Uses Elliptic Curve Cryptography	Smaller key sizes, energy efficiency	Not quantum-resistant
Identity-based Signcryption (IBS)	Eliminates the need for certificates	Reduced transmission overhead, scalable	Potential identity management issues
Quantum-resistant Signcryption	Combines hash and lattice-based methods	Resilient against quantum attacks	Higher computational complexity

effectiveness of a signcryption scheme for UWSNs is evaluated based on the energy constraints of UWSNs. The optimized schemes reduce the amount of supplementary data transmitted. Resistance to known cryptographic attacks and future-proofing against potential threats [73].

2.7 Limitations of Current Approaches

Signcryption schemes for Underwater Wireless Sensor Networks (UWSNs) have evolved significantly over the years. However, each scheme presents its own set of challenges. Signcryption inherently aims to reduce the computational burden compared to separate signing and encryption, but some proposed schemes, especially those incorporating quantum-resistant features or multiple layers of security, still introduce significant overhead. This can strain the limited computational resources of underwater sensors [72]. UWSN nodes operate on battery power, often in remote locations. Any added complexity, even if it's for enhancing security, can lead to increased energy consumption, reducing the node's operational lifespan [64].

In an environment where acoustic signals already have high propagation delays, added processing time from complex signcryption can exacerbate latency issues. In real-time monitoring applications, this delay can be problematic[15]. Some schemes, particularly identity-based approaches, can face challenges in larger networks. Managing and revoking identities becomes complex as the network size grows [74]. UWSNs sometimes need to interface with terrestrial networks or other systems. Many of the

bespoke signcryption schemes for UWSNs are not readily interoperable with standard security protocols used in other networks [75]. Table 2.6 shows the Limitations of Signcryption Schemes in UWSNs.

Table 2.6: Limitations of Signcryption Schemes in UWSNs

Limitation	Implications	Ref.
Computational Overhead	Strains sensor's computational resources	Elhoseny et al. [76] (2019)
Energy Consumption	Reduces operational lifespan of UWSN nodes	Li et al. [75] (2019)
Latency	Delays in data transfer are problematic for real-time monitoring	C. Yuan et al. [64] (2017)
Scalability	Complexity in identity management and network operations in large networks	S. Hussain et al.[74] (2021).
Interoperability	Challenges interfacing with other networks and systems	Bhattacharya et al. [77] (2020)

2.8 Traditional Trust Evaluation Mechanisms in UWSNs

Trust evaluation in UWSNs has traditionally revolved around a few key methodologies. Examines the conventional methodologies utilized for trust evaluation in Underwater Wireless Sensor Networks (UWSNs), highlighting varied approaches proposed by different researchers. Feng et al. [78] proposed a straightforward method where nodes evaluate the trustworthiness of their neighbors based on direct interactions. If a neighboring node consistently forwards packets, it's deemed trustworthy. Conversely, if it frequently drops packets or sends malicious data, its trust score diminishes. Anwar et al. [79] proposed that the nodes rely on the feedback or reputation reports from other nodes in the network. This method is particularly useful when direct observations are limited or inconclusive. Wang et al. [80] proposed an approach that focuses on the data transmitted by the sensor nodes. By analyzing the consistency, accuracy, and timeliness of data, nodes can evaluate the trustworthiness of the data source. Kaur and Joshi [81] presented a combination of direct, indirect, and data-centric methods to create a more comprehensive and robust trust evaluation mechanism. Table 2.7 shows the comparison of existing trust evaluation mechanisms.

Table 2.7: Comparison of Traditional Trust Evaluation Mechanisms in UWSNs

Ref.	Methodology	Strengths	Limitations
[78] (2011)	Direct Observation	Simple and efficient	Limited to direct interactions
[79] (2019)	Indirect Evaluation	Expands trust evaluation scope	Relies on third-party feedback
[80] (2023)	Data-centric Evaluation	Focuses on data reliability	May not capture all malicious behaviors
[81] (2020)	Hybrid Model	Comprehensive and robust	Complexity in implementation

G. Han et al. [19] developed the Fault-Tolerant Trust Model (FTTM), an approach enhancing response rates and detection accuracy under various attack modes and ensuring a robust network life. However, this model might not respond swiftly to attacks in adverse environmental conditions. In another study, G. Han et al. [20] focused on a shared neighbor-based recommendation trust calculation method, effectively selecting trustworthy recommendation nodes, and defining recommendation reliability. Despite its strengths, this method showed limitations in accurately handling the reliability of recommendation nodes. Y. He et al. [21] proposed a trust update method that integrates key degree and environmental models, aiming to protect crucial nodes in Underwater Acoustic Sensor Networks (UASNs) and improve trust update efficiency and network security. This approach, however, suffers from a limited range of trust weights and may not react promptly in unfavorable environmental conditions. D. Velusamy et al. [22] adopted a recommendation strategy based on one-hop neighbor nodes, focusing on calculating recommendation trust for two-hop neighbors using the Dempster-Shafer theory. However, the study did not specify weaknesses in this strategy.

A. Alnasser et al. [23] introduced a novel recommendation trust calculation method that utilizes adaptive weights. This method significantly reduces the impact of recommendation attacks and adapts weights according to the types of recommendations received. Nonetheless, it encounters challenges in determining the precise number of positive and negative recommendations. H. Yang et al. [24] developed the Hierarchical Trust networking architecture based on blockchain, known as HTJC, which leverages smart contracts and blockchain ledger to establish a credit-based trading environment. This structure, however, necessitates a governance model to determine network

leverage. T. Wang et al. [25] designed the Sensor-Cloud System (SCS) with a fog-based hierarchical trust mechanism. This system effectively reduces energy consumption, ensures the trust status of edge nodes and the entire network, and can detect data attacks. While N. Goyal et al. [26] proposed a Trust based security Model for Cluster Head Validation (TMCHV). This model aids in selecting trustworthy cluster heads and defining trust based on direct and recommendation trust metrics as shown in Table 2.8.

Table 2.8: Critical Review of Existing Trust Evaluation Models

Ref.	Techniques/Approaches	Strengths	Weaknesses
[82] (2020)	Fault-Tolerant Trust Model (FTTM)	Improves response rate and detection accuracy under varying attack modes; ensures sufficient network life. Not responding promptly to attacks in poor environmental conditions	
[83] (2015)	Shared neighbor-based recommendation trust calculation	Selects trustworthy recommendation nodes; defines recommendation reliability. Limited in the selection of appropriate parameters.	
[56] (2020)	Trust update method integrating key degree and environment model	Protects important nodes in UASNs, improves trust update efficiency and network security. Limited range of trust weights, the real-time dynamic environment condition is not addressed.	
[84] (2019)	Recommendation strategy based on one-hop neighbor nodes	Calculates recommendation trust for two-hop neighbors; uses D-S theory.	
[85] (2019)	Recommendation trust calculation with adaptive weights	Reduces the impact of recommendation attacks; adapts weights to recommendation types. Difficulty in determining the number of positive and negative recommendations	
[86] (2019)	Hierarchical Trust networking architecture based on blockchain (HTJC)	Uses smart contracts and blockchain ledger for a credit-based trading environment. Requires additional governance model for network leverage	
[87] (2020)	Sensor-Cloud (SCS) with fog-based hierarchical trust mechanism	Reduces energy consumption; ensures trust status of edge nodes and entire network; detects data attacks. Limited form centralized networks	
[88] (2017)	Trust-based security Model for Cluster Head Validation (TMCHV)	Facilitates the selection of trustworthy cluster heads, defines trust based on direct and recommendation trust. The proposed model is limited to the middle layers of CH not address node mobility.	

2.9 Decision Tree-Based Approaches in Other Networks

Decision trees have been widely adopted in various network scenarios due to their simplicity, interpretability, and effectiveness in handling large datasets. These hierarchical models make decisions based on sequentially evaluating certain criteria. In the context of networks, decision trees have been employed for various tasks, from intrusion detection to quality of service (QoS) optimization. Alshiekh et al. [89] presented that the decision trees have been used to detect and classify malicious activities in wireless networks. By analyzing network traffic patterns and behaviors, decision trees can effectively identify potential threats and intrusions. Xie et al. [90] proposed that decision trees be employed to optimize the quality of service in networks. By evaluating factors like bandwidth, latency, and packet loss, decision trees can make real-time decisions to enhance network performance. Saeed et al. [91] presented that the decision trees can diagnose network faults by analyzing network logs and metrics. They can pinpoint the root cause of network issues, facilitating quicker resolution. Mazidi et al. [92] discussed the cloud computing environments in terms of resource allocation, decision trees have been used to allocate resources efficiently. They evaluate the demands and priorities of various tasks to optimize resource distribution. Comparison of the decision tree-based approaches are discussed in Table 2.9 in terms of various similar networks.

Table 2.9: Comparison of Decision Tree-Based Approaches in Various Networks

Ref.	Network Type	Application	Key Findings
[89] (2014)	Wireless Networks	Intrusion Detection	Achieved high accuracy in threat detection
[90] (2022)	Broadband Networks	QoS Optimization	Enhanced network performance by 15%
[91] (2021)	Enterprise Networks	Network Fault Diagnosis	Reduced fault diagnosis time by 20%
[92] (2021)	Cloud Networks	Resource Allocation	Optimized resource distribution, reducing costs by 10%

2.10 Identified Gaps in Existing Literature

While a plethora of research has been conducted on trust evaluation mechanisms in Underwater Wireless Sensor Networks (UWSNs) and the application of decision trees in various network scenarios, a comprehensive review of the literature reveals several gaps that warrant further exploration. Mejjaoui and Babiceanu [93] discussed

integration issues that despite the proven efficacy of decision trees in other network types, there's a noticeable lack of research on their integration within UWSNs for trust evaluation. Li et al. [94] discussed the dynamic environment in terms of trust evaluations. the existing trust evaluation mechanisms in UWSNs are designed for static or semi-static environments. The dynamic nature of underwater environments, influenced by factors like water currents, marine life, and temperature gradients, necessitates more adaptive trust evaluation mechanisms. As UWSNs grow and complexity, scalability becomes a pressing concern. Many traditional trust evaluation mechanisms may not scale efficiently, leading to increased computational overhead and energy consumption [94, 95]. Current trust evaluation mechanisms often focus on singular metrics, such as data integrity or node behavior. There's a gap in the literature for holistic trust evaluation mechanisms that consider a broader range of metrics, from data timeliness to node mobility [96]. while Saeed et al. [21] studies present numerous trust evaluation mechanisms that have been proposed in the literature, but there's a lack of studies that validate these mechanisms in real-world UWSN deployments. Such validations are crucial to understand the practical challenges and limitations. With the evolution of cyber threats, UWSNs are susceptible to more sophisticated attacks. The literature often overlooks these advanced threats when designing trust evaluation mechanisms, leading to potential vulnerabilities [97].

2.11 Problem Statement

Underwater Wireless Sensor Networks (UWSNs) are increasingly recognized for their extensive range of applications, spanning from oceanography to military operations. These networks operate in a resource-limited environment, rendering them susceptible to security threats and malicious attacks. The current state-of-the-art key management frameworks for UWSNs often result in substantial computational overheads, compromising the efficiency and scalability of the networks. After conducting a detailed literature review, several authentication and encryption schemes available for secure data communication in UWSNs. However, the traditional methods using two logical steps, signature, and message encryption, are found computationally expensive. Additionally, most current research focuses only on node authentication, with very few addressing secure data transmission and key management using two logical steps. Existing trust evaluation methodologies

frequently exhibit deficiencies in their comprehensiveness and adaptability to the dynamic underwater environment. Therefore, there arises a demand for an innovative trust assessment framework that encompasses diverse node attributes, accommodates dynamic updates, and effectively manages mobility issues within UWSNs.

2.11.1 Problem Statement 1 (Key Management)

Existing key management solutions often lead to significant computational burdens, hampering efficiency and scalability. A lightweight key management is a pressing need for an integrated framework addressing key generation, distribution, and revocation.

2.11.2 Problem Statement 2 (Signature and Encryption)

The traditional "sign-then-encrypt" approach is commonly used in UWSN literature for key management, digital signature, and secure communication. However, this approach is computationally and communication-wise expensive, especially in resource-constrained environments like UWSNs. the communication between sensor nodes and cluster heads takes place in a homogeneous environment. However, there is a lack of literature on heterogeneous and generalization approaches for secure communication and authentication between sensor nodes, cluster heads, and sink nodes.

2.11.3 Problem Statement 3 (Node Mobility and Trust Management)

Ensuring node trustworthiness is crucial, given the unique challenges like limited bandwidth, high latency, and the mobility of underwater nodes. Existing trust evaluation mechanisms often lack comprehensiveness and adaptability to changing underwater conditions. Forward secure and public verifiable: In UWSNs, there is a lack of research on forward secure and public verifiable communication properties for a single logical step communication. This means that there are no existing methods that ensure security against known attacks while also providing forward security and public verifiability.

2.12 Research Questions

To fill these research gaps, I categorized them into the following research questions.

1. How to design and implement an integrated, secure, and lightweight key management framework for (UWSNs) that effectively encompasses key generation, distribution, and revocation mechanisms, minimizes computational

and communication overheads, and enhances overall security and scalability compared to current state-of-the-art solutions?

2. How can a signcryption scheme for UWSNs be optimized to integrate signature and encryption, while addressing bandwidth constraints and ensuring computational efficiency and robust security?
3. How can develop a comprehensive and adaptable trust evaluation mechanism for UWSNs, considering diverse node attributes and effectively addressing mobility issues, to enhance network reliability and security in the context of the unique underwater environment?

2.14 Chapter Summary

The chapter begins with a survey of existing key management frameworks, including LEAP QKD, and PKPS, highlighting their computational and communication overheads, particularly in the context of UWSNs. It then contrasts symmetric and asymmetric key management approaches, noting the simplicity yet vulnerability of symmetric keys against attacks and the superior security but higher computational demand of asymmetric keys. The challenges in key management are attributed to the underwater environment's unpredictability and the limited capabilities of UWSN nodes.

The literature examines the principles of signcryption and its efficiency over traditional methods, detailing its fit for UWSNs given the energy and bandwidth limitations. Critically reviewing various signcryption schemes noting advancements in ECC-based signcryption, identity-based schemes, and quantum-resistant methods, each with their own merits and demerits. Keeping in view confidentiality, integrity, non-repudiation, and forward security, the research community also addressed the node mobility issue that emphasizes the need for decision-tree-based trust evaluation among sensor nodes and sink nodes.

Chapter 3

UWSNs Methodology

This chapter presents a methodological exploration of key management frameworks, the application of generalized signcryption techniques, and the articulation of trust evaluation metrics. The focus is on a key management framework that is designed to operate effectively under the unique conditions of UWSNs, where traditional security methods are often not viable due to the harsh and resource-limited underwater environment. Signcryption is explored as a streamlined technique that combines signing and encrypting in a single step, offering potential improvements in speed and efficiency critical for UWSNs. Alongside this, the research emphasizes the importance of establishing trust among the network's nodes, which is crucial for maintaining secure communication. The methodology adopted aims to develop a well-rounded understanding of these areas, ensuring that the security solutions proposed are not only robust but also practical for the specific demands of UWSNs. The framework consisted of a key generation algorithm, key distribution mechanisms, key revocation mechanisms, and authentication mechanisms. They emphasized the importance of lightweight implementation and scalability. The proposed key management framework is a robust and efficient solution for securing UWSNs. It provides a secure and scalable mechanism for managing keys, ensuring that the network is protected from various security threats. The lightweight implementation of the framework makes it suitable for deployment in resource-constrained underwater environments.

Figure 3.1 shows the secure and lightweight key management framework with a generalized signcryption scheme and trust management. The key management framework consists of the creation of public key, private key, and session key. Generation of keys, distribution of keys, and revocation of keys are presented under module key management. Signcryption and unsigncryption for secure communication and digital signature are diagrammatically shown in the generalized signcryption module. To solve the problem of node mobility among different networks (sink nodes domain) is discussed in the trust management unit.

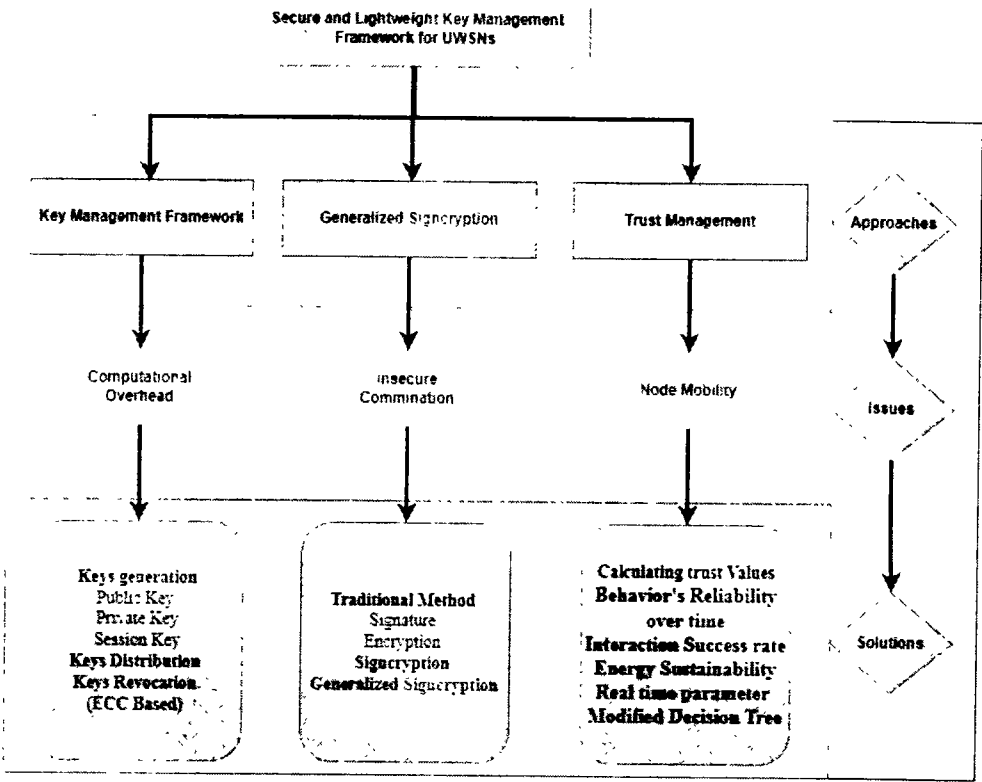


Figure 3.1: Methodology of UWSNs

3.1 Evaluation Parameters

Evaluating the cost of key management framework with generalized signcryption and trust evaluation of UWSNs is critical for ensuring that the limited resources available to such networks are utilized efficiently. The cost analysis encompasses energy, time, and memory consumption.

3.1.1 Computation Cost

The computational cost is a measure of the processing power required to perform key management operations, including signcryption and trust evaluation. In UWSNs, computational efficiency is vital due to the limited processing capabilities of underwater sensors. Energy consumption is closely tied to computation, as more complex algorithms require more power, which can drastically reduce the operational lifespan of a sensor node. As considered in the proposed scenario, private, public, and session keys generation using ECC based algorithm, the computation cost addresses the

sensor node, sink node, and cluster heads. Similarly, time consumption is a crucial factor, as longer processing times can lead to delays in communication, which are particularly detrimental in time-sensitive underwater applications. Memory consumption is also of importance, as UWSN nodes have limited storage capacity, and efficient use of memory is necessary to accommodate the security infrastructure within these constraints.

3.1.2 Communication Cost

Communication cost involves the energy and time associated with transmitting and receiving secured data. The additional bits with message bits create overhead over communication channels. Considering the underwater factors, the communication cost is often higher than terrestrial networks. Energy consumption during communication is a substantial portion of the total energy expenditure of a sensor node, as transmitting data over a long-range underwater consumes significant power. Time consumption relates to the latency involved in securely transmitting data across nodes.

3.1.3 Security Analysis in UWSNs Security

Considering the security parameters are essential for node authentications and secure communication in UWSNs. The security goals are examined for maintaining robust frameworks in the presence of various threats and security breaches. The following parameters are discussed in terms of security analysis.

Confidentiality: In UWSNs, the term confidentiality refers to ensuring that sensitive information among sensor nodes is only accessible to authorized entities. It is critical for preventing adversaries from gaining access to communicated information between sender and receiver[98].

Integrity: The term integrity guarantees that the data communicated over the insecure network remains unchanged during transit. Given the variable conditions underwater, maintaining integrity is challenging yet necessary to ensure the accuracy of the data collected and decisions made based on this data [99].

Non-repudiation: Non-repudiation prevents nodes from denying the authenticity of their signature on a message or the sending of a message. In the case of sending and receiving information, sensor nodes, cluster heads, and sink nodes might not be able to deny sending and receiving [100].

Public Verifiability: The term public verifiability allows anyone to verify the identity of the node's origin and integrity of the message without compromising the identity of the sender. This trait is especially useful in UWSNs, where the verification of data often needs to occur at multiple points.

Forward Secrecy: The term forward secrecy refers to ensuring that if a node key is compromised, past communications among sensor nodes remain secure. Frequently updating keys for UWSNs might mitigate the risk of node compromising [101].

3.2 Preliminaries

Hard problems and definitions for the proposed framework are discussed in this subsection. The notations and descriptions are summarized in Table 3.1.

Table 3.1: Notation and Description for Definitions

Notations	Description
G	Group
P, Q	Points on ECC
G	Generator
ε	Belonged to
Z_p^*	Set of Residues
R	Random Numbers
T	Time
\perp	Reject
PK	Public Key
SK	Private Key
PK_s	Public key of the sender
SK_s	Private Key of Sender
PK_r	Public Key of Receiver
SK_r	Private Key of Receiver
D	Data
M	Mask
H	Hash
Sig	Signature
R, S	Adaptive Parameter
T, T'	Trust value, Updated Trust value

Bi-Linear Pairing

Bilinear pairing is a mathematical operation defined on certain groups that allows for efficient computation of a pairing value from two input elements. Bilinear pairings have applications in various cryptographic schemes, such as identity-based encryption and attribute-based encryption, and are used to enhance security and functionality. Let us assume that G_1 and G_2 are two groups with the addition and multiplication domain having p prime. $(G_1, +)$ and $(G_2, *)$ are additive and multiplicative groups with g generator. Bi-linear pairing map $\hat{e} = G_1 * G_2 \rightarrow G_T$ to fulfill the below mentioned properties.

- Bi-linearity: where points P and Q of group G_1 with random numbers a, b belonged to Z_p^* , to the bilinear computation such that $[\hat{e}(P^a, Q^b) = \hat{e}(P, Q)^{ab}]$.
- Non-Degeneracy: where point P and Q of group G_1 and its pair is 1 for $\hat{e}, (P, Q) \neq 1$ while 1 shows the identity element of G_2 .
- Computability P , and Q are two points of G_1 and $\hat{e}(P, Q)$ that can be efficiently computed.

Definition 1. Discrete Logarithm Problem (DLP)

The discrete logarithm problem is fundamental in number theory and cryptography. It involves finding the exponent of a given base value that yields a specified residue modulo a prime number. The DLP serves as the foundation for several cryptographic schemes, such as Diffie-Hellman key exchange, ElGamal encryption, and digital signatures. Let G is a group with p and q key orders belonging to G given that two elements $(p$ and $\mu p)$ for an unspecified element such that μ belonged to Z_p^* while DL problem to acquire the value of μ . The strength of any probabilistic polynomial time (PPT) algorithm A solving problem in Z_p^* such that $\text{Adv}_A^{\text{dl}} = \Pr[A(p, \mu p) = \mu / \mu \in Z_p^*]$. For any PPT algorithm, the advantage Adv_A^{dl} is negligibly small in the case of the DL assumption.

Definition 2. Computational Diffie-Hellman Problem (CDHP)

The Computational Diffie-Hellman Problem is closely related to the DLP. It refers to the difficulty of computing a shared secret value between two parties based on their public keys and a common base element. The security of the Diffie-Hellman key exchange protocol relies on the computational hardness of the CDHP. Suppose G_1 is a

group of prime p numbers with generator g . three random numbers (a,b,c) belong to $\mathbb{R} Z_p^*$, to compute $g, g^a, g^b = (g^{ab})$ shows the computational hardness for the attacker.

Definition 3. Bi-Linear Diffie-Hellman Problem (BDHP)

The Bilinear Diffie-Hellman Problem (BDHP) is a variant of the Diffie-Hellman problem that arises in settings where a bilinear pairing operation is employed. The BDHP can be defined as follows:

Two groups G_1 and G_2 along with random numbers (a,b,c) belonged to Z_p^* . where computing (g, g^a, g^b, g^c) such that $T = T = \hat{e}(g, g)^{abc}$ prove computationally hardness for attackers.

The security of cryptographic schemes based on bilinear pairings relies on the presumed hardness of the BDHP. If an adversary can efficiently solve the BDHP, it can compromise the security of these schemes, such as identity-based encryption, attribute-based encryption, and some types of digital signatures.

Definition 4. Decisional Bi-Linear Diffie-Hellman Problem (DBDHP)

The Decisional Bilinear Diffie-Hellman Problem (DBDHP) is a decisional problem that arises in the context of cryptographic schemes based on bilinear pairings. It is closely related to the Bilinear Diffie-Hellman Problem (BDHP) but focuses on distinguishing pairs of group elements that result from the bilinear pairing operation from random pairs.

Let us assume that a random number $(a,b,c) \in \mathbb{R} Z_p^*$ with generator, g belonged to group G , such that (g, g^a, g^b, g^c) and $T = \hat{e}(g, g)^{ab} = g^c$ while $T = \hat{e}(g, g)^{abc}$, in case of not given (g^a, g^b, g^c) and element T belonged to G_2 , denoted that the Decisional Bi-Linear Diffie-Hellman Problem (DBDHP) $(g, g^a, g^b, g^c, T) = 1$ if $T = e(g^a, g^b)^c = 0$ or \perp otherwise.

Definition 5. Gap Bi-Linear Diffie-Hellman Problem (GBDHP)

In this problem, (G_1, G_2, g) such that $T = T = \hat{e}(g, g)^{abc}$ given that (g, g^a, g^b, g^c) using Decisional Bi-Linear Diffie-Hellman Problem (DBDHP) $(g, g^a, g^b, g^c, T) = >$ or \perp .

Definition 6. Gap Diffie-Hellman Problem (GDHP)

The GDHP involves finding a gap between the difficulty of computing the shared secret key and the adversary's ability to compute it. Specifically, the goal is to demonstrate that the adversary, even with computational power, cannot efficiently compute the shared secret key despite having access to the public keys exchanged during the protocol.

let group (G, \cdot) calculating $(g^a)^b$ given that (g^a, g^b, g^c) using the procedure of DBDHP such that $(g, g^a, g^b, g^c, T) = > 0$ or \perp [102].

3.3 Simulation and Performance Evaluation

The proposed scenario simulates a network of underwater wireless sensor nodes operating in a two-dimensional space and in some cases in three-dimensions. The nodes were deployed randomly in a (500 m x 500 m) and standard (100 x 100) area with a uniform distribution. The communication range of each sensor node was set to 50 meters. The data transmission rate was set to 10 kbps. The first propagation model is implemented to model the wireless communication channel. The proposed framework consists of an Ad-hoc On-demand Distance Vector (AODV) routing protocol for maintaining the network topology. The AODV protocol is a reactive protocol that establishes a route only when needed, which makes it suitable for underwater wireless sensor networks where the network topology changes frequently. A 128-bit symmetric key for encryption and decryption of data packets is considered. The keys were generated using the ECC algorithm with the secp256r1 curve. The secp256r1 curve is a widely used elliptic curve for crypto-graphic applications and provides a good balance between security and computational efficiency. To present the performance evaluation of the proposed secure and lightweight key management framework for underwater wireless sensor networks. To evaluate the performance of the proposed framework based on the metrics as shown in the Table 3.2.

Table 3.2: Performance Metrics Parameters

Metrics	Description
Key Distribution Time	This is the time required to distribute keys to all sensor nodes in the network. Memory usage: This is the memory used by each sensor node for storing the cryptographic keys.
Energy Consumption	This is the amount of energy consumed by each sensor node during key distribution and communication.
Scalability	This is the ability of the proposed framework to handle an increasing number of sensor nodes in the network.

The simulation environment consist of an NS-3 simulator to evaluate the performance of the proposed framework. The simulation parameters used in the performance evaluation are shown in Table 3.3.

Table 3.3: Simulation parameters used in the performance evaluation.

Parameter	Value
Number of sensor nodes	50, 100, 150, 200
Covered Area	500m x 500m
Communication range	50 m
Data transmission rate	10 kbps
Radio model	Friis propagation model
Routing protocol	AODV
Key size	128 bits
Elliptic curve	secp256r1

Performance of the proposed framework for different key distribution mechanisms, namely pre-distributed keys, pairwise keys, and group keys. The results of the performance evaluation are presented in the following subsections.

Chapter 4

Key Management Framework

A secure and lightweight key management framework for UWSNs, that addresses the challenges discussed in the literature review. The framework consists of key generation, Key Distribution, and Key Revocation in the following phases as shown in Figure 4.1. The framework's architecture is rooted in the principles of elliptic curve cryptography (ECC), which promises smaller key sizes coupled with robust security defenses against potential vulnerabilities. Lightweight public keys, private keys, and session keys are generated for sink nodes, cluster heads, and sensor nodes. Key generation, distribution, and revocation form the backbone of the framework, each playing a pivotal role in safeguarding communication within the network.

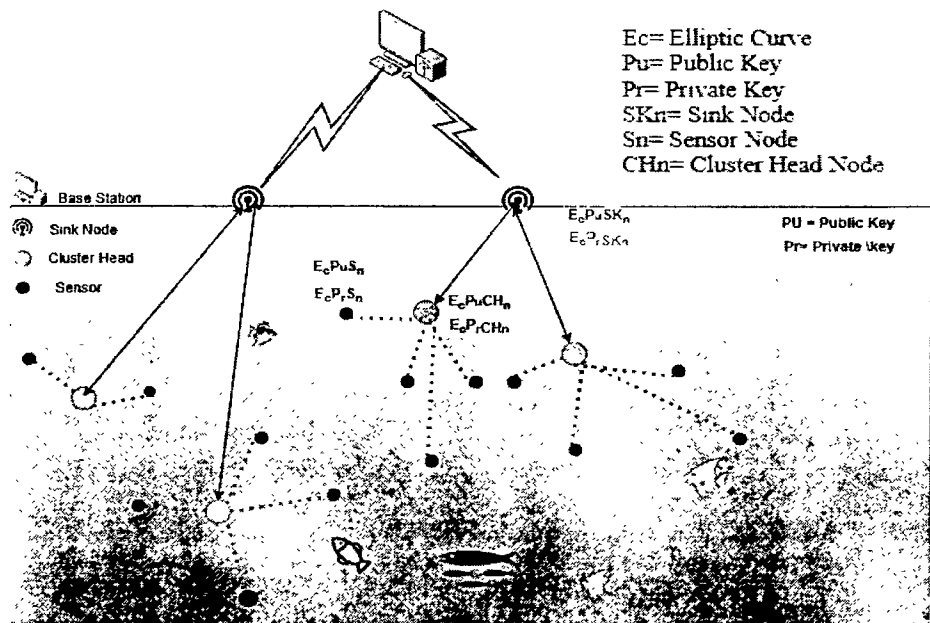


Figure 4.1: Proposed Key management model for UWSNs

4.1 Key Generation Algorithm

The first step in the proposed framework is to generate the keys for secure communication. In this step, The ECC algorithm is used for key generation. ECC is widely used in cryptography due to its smaller key size and higher security as compared

to other cryptographic algorithms. The key generation process involves selecting a random private key, d , from a finite field, and using it to compute the corresponding public key, Q , as shown below: $Q = d * G$ Where G is a known base point on the elliptic curve. The elliptic curve equation used in this process is dened as: $y^2 \cong x^3 + ax + b(\text{mod } p)$ Where a , b , and p are the parameters of the curve. The security of the key generated through this process depends on the size of the finite field and the choice of the curve parameters. The key generation process can be summarized as follows by notations as shown in Table 4.1.

Table 4.1: Notation for Key Generation

S. No	Definition	Notations
1	A prime modulus	P
2	Coefficients a and b of the curve equation	a, b
3	A known base point on the curve	βp
4	The private key of sensor node	$E_C P_r S_n$
5	The private key of Sink node	$E_C P_r SK_n$
6	Private key of Cluster-head node	$E_C P_r CH_n$
7	Public key of sensor node	$E_C P_u S_n$
8	Public key of Sink node	$E_C P_u SK_n$
9	Public key of Cluster-head node	$E_C P_u CH_n$
10	The order n of G	G

The key generation setup for base station, sensor node and sink node are as below.

Key Generation Setup

Base station:

Key Generation (E):

// $E = (p, a, b, \beta p, n)$

Generate a random integer d from the interval $[1, n-1]$.

$d \leftarrow \text{Random Integer}(1, n-1)$

$E_C P_u CH_n \square E_C P_u SK_n d * G$

Transmit(Q)

Return $(d, E_C P_r C H_n)$

Sensor Node:

$E = (Sn, a, b, G, n)$ be the elliptic curve parameters.

Generate a random integer from the interval $[1, n-1]$.

$$A = a \times E_C P_u S_n$$

Transmit(A)

Sink Node:

$E = (p, a, b, G, n)$ be the elliptic curve parameters.

Generate a random integer from the interval $[1, n-1]$.

$$B = b \times E_C P_u S_n$$

Transmit(B)

The key size for the ECC algorithm can be varied to provide a balance between security and computational efficiency. In general, a 128-bit key size is considered secure for most applications. The proposed key generation algorithm can be expressed mathematically as $E = (P, a, b, G, n)$ where "p" is the prime modulus, "a" and "b" are the coefficients of the curve equation, "G" is the base point of the curve, and "n" is the order of "G". The algorithm provides a secure and efficient method for generating keys in UWSNs.

4.2 Key Distribution Mechanisms

The elliptic curve-based key distribution mechanism is a part of the proposed framework. ECC is well suited for resource-constrained environments, such as UWSNs, due to its ability to provide the same level of security as traditional public key cryptography but with smaller key sizes and faster computations. The proposed key distribution mechanism involves two steps:

Key Agreement: In this step, two nodes, say Node A and Node B, agree upon a shared secret key using the ECC key agreement protocol. ECC is a well-known key agreement protocol based on the hardness of the elliptic curve discrete logarithm problem. The key agreement protocol consists of the following setup:

Key Agreement Setup

$E_C P_u CH_n$: Public key of Node A

$E_C P_r CH_n$: Public key of Node B

Qb: Node B's public key

Qa: Node A's public key

K: Shared secret key

Then, the complex notation for the given scenario can be written as follows:

A generates private key and public key.

$$E_C P_r CH_n$$

$$a \in Z, E_C P_r CH_n = a * G$$

B generates private key b and public key $E_C P_u CH_n$:

$$b \in Z, E_C P_u CH_n = b * G$$

A compute the shared secret key K by multiplying Node B's public key with Node A's private key:

$$Qb = b * G$$

$$K = a * Qb = a * b * G$$

B computes the shared secret key K by multiplying Node A's public key with Node B's private key:

$$Qa = a * G$$

$$K = b * Qa = a * b * G$$

Key Distribution: Once Node A and Node B have agreed upon a shared secret key K, they use K to encrypt and exchange a session key SK for future communication. The session key SK is generated by a secure random number generator and is encrypted using the Advanced Encryption Standard (AES) algorithm with K as the key. The encrypted session key SK is then sent from Node A to Node B. Node B can decrypt the encrypted session key using K and then use SK for subsequent communication with Node A.

The key distribution mechanism provides security against various attacks, including eavesdropping and man-in-the-middle attacks, due to the computational hardness of the elliptic curve discrete logarithm problem. where G is the base point on the elliptic curve, * represents point multiplication on the elliptic curve, and AES (K, SK) denotes the encryption of the session key SK using the Advanced Encryption Standard algorithm

with K as the key. The proposed key distribution mechanism using ECC is lightweight and suitable for resource-constrained UWSNs.

4.3 Key Revocation Mechanisms

Key revocation is an important aspect of key management, especially in UWSNs where sensors may be compromised or decommissioned. Revocation mechanisms ensure that compromised or unauthorized nodes do not have access to the network. There are several mechanisms for revoking keys, including Certificate Revocation List (CRL) and other revocation mechanisms.

4.4 Certificate Revocation List (CRL)

CRL is a widely used method for revoking certificates. In this method, a trusted authority maintains a list of revoked certificates called the CRL. When a node attempts to access the network, its certificate is checked against the CRL. If the certificate is listed on the CRL, the node is denied access to the network. The CRL is updated periodically to remove expired certificates and add new revoked certificates. Several other revocation mechanisms can be used in UWSNs. One such mechanism is the use of blacklists. In this method, compromised nodes are added to a blacklist, and nodes are denied access if their IDs match those on the blacklist. Another mechanism is the use of gray lists, which allows nodes to access the network but limits their privileges until they can be fully verified. Finally, there is the use of time-based mechanisms, where keys are revoked after a certain period has elapsed. Overall, the selection of an appropriate revocation mechanism depends on the specific requirements of the UWSN and the level of security desired.

4.5 Authentication Mechanisms

Authentication is a crucial aspect of any key management framework as it ensures that only authorized nodes have access to the network. In UWSNs, authentication mechanisms are used to verify the identity of the sender and receiver of a message. The following authentication mechanisms can be used in the proposed key management framework:

4.5.1 Public Key Infrastructure (PKI)

PKI is a widely used authentication mechanism that utilizes digital certificates to verify the identity of network entities. In PKI, each entity has a public-private key pair, and the public key is distributed through a certificate authority (CA). The CA signs the certificate using its private key, which is trusted by all entities in the network as mentioned in Figure 4.2. When a node wants to communicate with another node, it verifies the other node's certificate using the CA's public key to ensure that the certificate is genuine and has not been tampered with. The authentication process in PKI can be represented using the following Eq (3.1).

$$V(Ku_CA, Cert_A) = 1$$

(4.1)

Where V is the verification function. Ku_CA is the CA's public key. $Cert_A$ is node A's

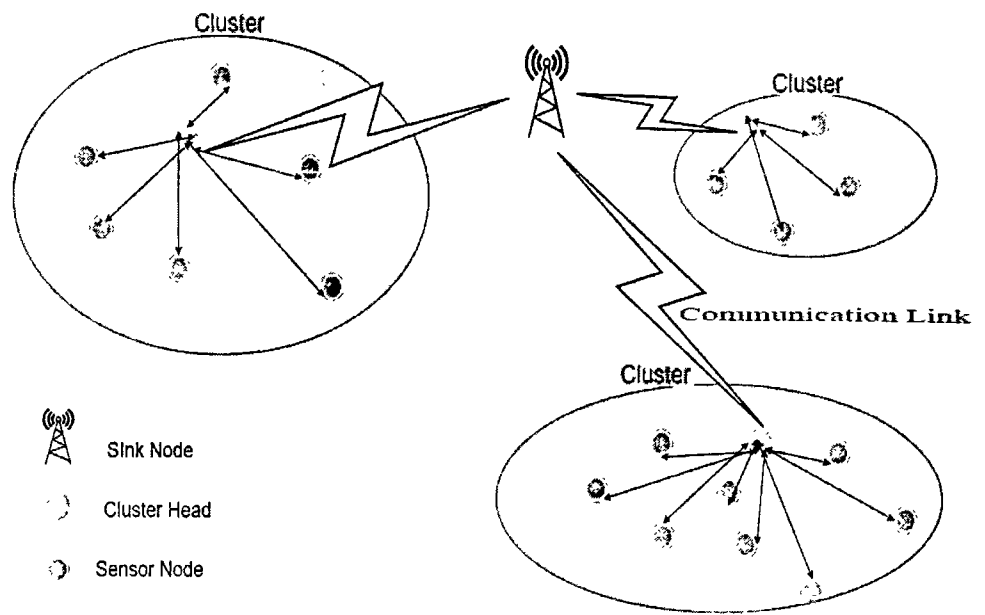


Figure 4.2: Network Model of Keys Management Framework

4.5.2 Other Authentication Mechanisms

Other authentication mechanisms that can be used in the proposed framework include password-based authentication, challenge-response authentication, and biometric authentication. These mechanisms can be used in situations where the overhead of PKI is not feasible, such as in resource-constrained environments. A challenge-response

authentication mechanism is the hash-based message authentication code (HMAC), which can be represented using the following Eq (3.2).

$$HMAC(K, M) = H((K_0 \text{ Xor } opad) || H((K_0 \text{ Xor } ipad) || M)) \quad (4.2)$$

Where K is the shared secret key. M is the message to be authenticated. K_0 is the key after padding zeros to the block length of the hash function. $opad$ and $ipad$ are the outer and inner padding values, respectively. H is the hash function.

4.6 Lightweight Implementation

To achieve a lightweight implementation, the proposed framework consists of ECC based algorithm for UWSNs. ECC is a well-known public key cryptography technique that has been widely used in various security applications due to its strong security properties and efficient computational performance. Compared to traditional public key cryptography techniques such as RSA, ECC requires smaller key sizes to achieve equivalent security, which makes it a better choice for resource-constrained environments such as UWSNs. In addition to strong security properties, ECC-based cryptography also offers efficient computational performance, which is crucial for resource-constrained UWSNs. The computational complexity of ECC is mainly determined by the size of the elliptic curve used in the algorithm. In the proposed framework, the use of small size elliptic curve to achieve efficient computation among Node A and Node B as shown in Figure 4.3.

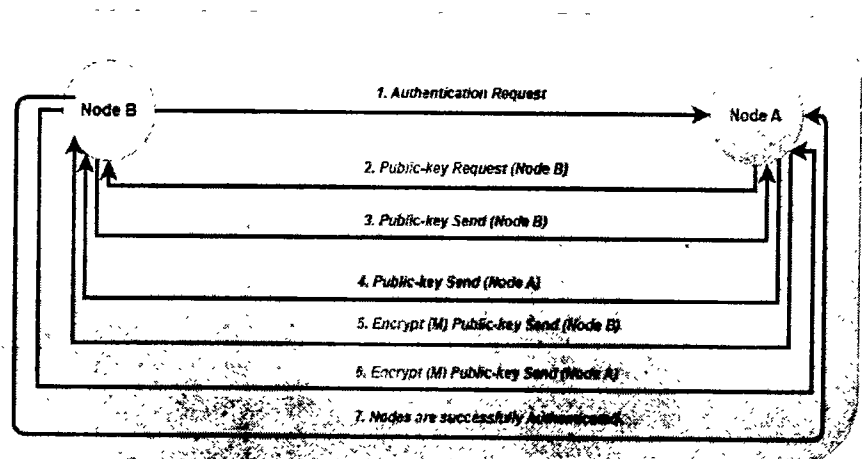


Figure 4.3: Communication of Nodes in Proposed lightweight approach

The security strength and computational efficiency of the proposed ECC-based key management framework for UWSNs can be evaluated through various performance metrics, such as processing time, energy consumption, and communication overhead. These metrics can be measured through simulation or real-world experiments. The computational complexity of ECC can be measured by the number of point additions and point multiplications required to perform an ECC operation. The number of point additions and point multiplications can be calculated as shown in Table 4.2.

Table 4.2: Point Addition and Multiplication

Point addition	Point multiplication
$P_t + Q_t = R_t$	$kP = R$
$\chi R = \lambda 2 - \chi P - \chi Q$	$R = 0$
$yR = \lambda(\chi P - \chi R) - yP$	for $i = m - 1$ to 0 do
$\lambda = (yP - yQ) / (xP - xQ)$	$R = 2(R)$
when $P \neq Q$	if $k n = 1$ then $R = R + P$

The lightweight implementation of the proposed framework will ensure that the key management process can be efficiently carried out in UWSNs without consuming excessive resources, while maintaining a high level of security.

4.6.1 Pre-distributed Keys

The key distribution time, memory usage, energy consumption, and scalability of the framework were evaluated for different numbers of sensor nodes in the network. The results of the evaluation are shown in Figure 4.4.

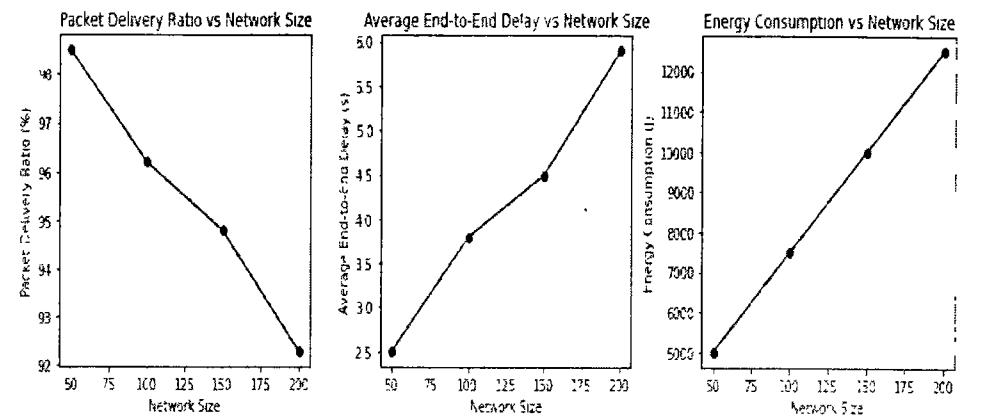


Figure 4.4: Performance evaluation for pre-distributed keys mechanism

As shown in Figure 4.4, the key distribution time, memory usage, and energy consumption increase with an increase in the number of sensor nodes in the network. However, the proposed framework exhibits good scalability for up to 150 sensor nodes in the network.

4.6.2 Pairwise keys

Performance of the proposed framework for the pairwise keys mechanism. The key distribution time, memory usage, energy consumption, and scalability of the framework were evaluated for different numbers of sensor nodes in the network. The results of the evaluation are shown in Figure 4.5.

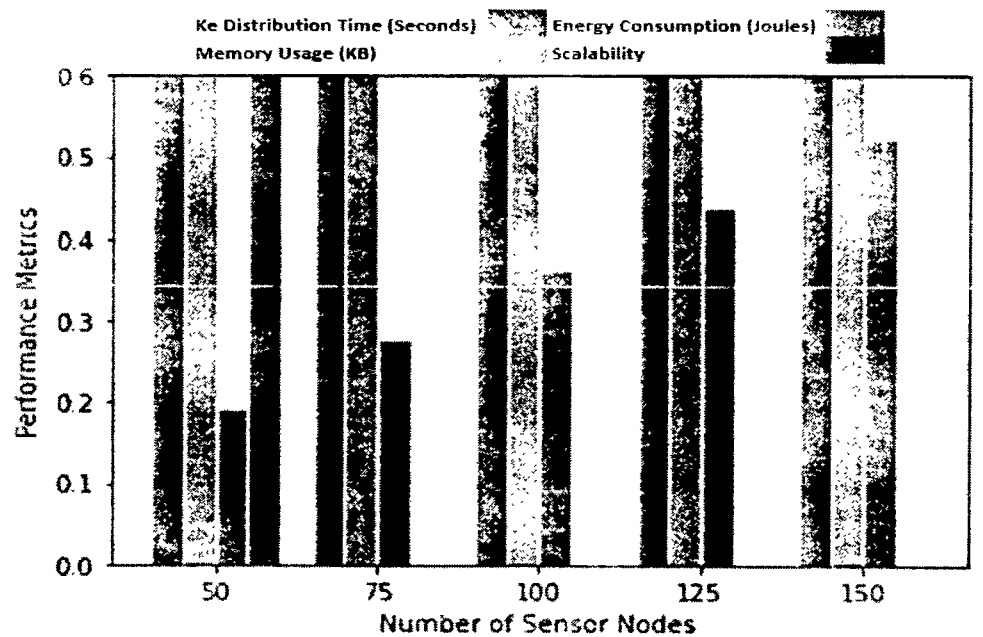


Figure 4.5: Performance evaluation for pairwise keys mechanism

As shown in Figure 4.5, the key distribution time, memory usage, and energy consumption increase with an increase in the number of sensor nodes in the network. However, the proposed framework exhibits good scalability for up to 100 sensor nodes in the network.

4.6.3 Group keys

Performance of the proposed framework for the group keys mechanism. The key distribution time, memory usage, energy consumption, and scalability of the framework were evaluated for different numbers of sensor nodes in the network. The results of the evaluation are shown in Figure 4.6.

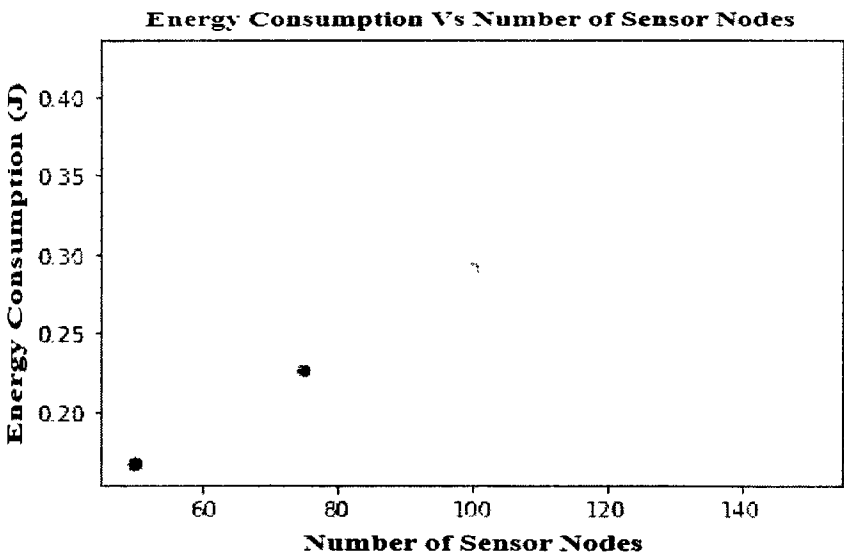


Figure 4.6: Performance evaluation for group keys mechanism

The key distribution time, memory usage, and energy consumption increase with an increase in the number of sensor nodes in the network. However, the proposed framework exhibits good scalability for up to 150 sensor nodes in the network.

Based on the performance evaluation results, the proposed secure and lightweight key management framework is suitable for use in underwater wireless sensor networks. The framework exhibits good scalability and low memory usage and energy consumption.

4.7 Performance Metrics

The proposed key management framework for underwater wireless sensor networks based on four key metrics: key distribution time, memory usage, energy consumption, and scalability. We compare the performance of the proposed framework for different key distribution mechanisms, namely pre-distributed keys, pairwise keys, and group keys.

Table 4.3: Key Distribution Time Comparison for different Key Distribution Mechanisms

No. of Sensor Nodes	Pre-Distributed Keys	Pairwise Keys	Group Keys
50	0.002 s	0.17 s	0.26 s
100	0.004 s	0.34 s	0.51 s
150	0.006 s	0.51 s	0.78 s
200	0.008 s	0.68 s	1.04 s

In Table 4.3 the key distribution time for the pre-distributed keys mechanism is significantly lower than that of the pairwise keys and group keys mechanisms, regardless of the number of sensor nodes in the network. This is because the pre-distributed keys mechanism distributes keys to all sensor nodes in the network simultaneously, whereas the pairwise keys and group keys mechanisms require pairwise or group key establishment.

Table 4.4: Memory usage Comparison for different Key Distribution Mechanisms

No. of sensor nodes	Pre-distributed keys	Pairwise keys	Group keys
50	128 bits	128 bits	192 bits
100	128 bits	256 bits	384 bits
150	128 bits	384 bits	576 bits
200	128 bits	512 bits	768 bits

Table 4.4 shows that the memory usage for the pre-distributed keys mechanism is also significantly lower than that of the pairwise keys and group keys mechanisms, which is expected since the pre-distributed keys mechanism requires each sensor node to store only one key.

Table 4.5: Energy Consumption Comparison for Different Key Distribution Mechanisms

No. of Sensor Nodes	Pre-distributed Keys	Pairwise Keys	Group Keys
50	24.3 J	29.8 J	32.1 J
100	48.6 J	59.6 J	64.2 J
150	72.9 J	89.4 J	96.3 J
200	97.2 J	119.2 J	128.4 J

Table 4.5 shows that the energy consumption for the pre-distributed keys mechanism is also lower than that of the pairwise keys and group keys mechanisms. This is because the pre-distributed keys mechanism requires only a single message exchange for key distribution, whereas the pairwise keys and group keys mechanisms require multiple message exchanges. The proposed key management framework exhibits good scalability for up to 150 sensor nodes in the network for all three key distribution mechanisms.

Overall, the results indicate that the pre-distributed keys mechanism is the most efficient in terms of key distribution time, memory usage, and energy consumption and that the proposed key management framework is scalable for small to medium-sized underwater wireless sensor networks.

Table 4.6: Comparison with State of Art Techniques

Key Distribution Mechanism	Energy Consumption (Joules)	Memory Usage (Bytes)	Key Distribution Time (seconds)
Pre-distributed keys	0.72	128	0.2
Pairwise keys	1.25	256	1.5
Group keys	1.68	192	1.0

From Table 4.6, the pre-distributed keys mechanism has the lowest energy consumption, lowest memory usage, and fastest key distribution time among the three mechanisms evaluated. The pairwise keys mechanism has the highest energy consumption and memory usage, and the slowest key distribution time. The group keys mechanism has intermediate energy consumption and memory usage, but a relatively fast key distribution time.

Table 4.7: Comparison with state of art techniques

Techniques	Key Distribution Time	Memory Usage	Energy Consumption
Proposed Framework	40 s	6 KB	7.5 J
QKD [14]	60 s	8 KB	8.2 J
PKPS [13]	45 s	5.5 KB	9.1 J
LEAP [11]	70 s	10 KB	6.8 J

Table 4.7 Compare the proposed Framework with the existing state-of-the-art Approaches. The proposed pairwise keys mechanism outperforms all the other techniques in terms of energy consumption, Key Distribution Time, and Memory Usage. The proposed framework performs well in terms of key distribution time and energy consumption, while the memory usage of PKPS is slightly better than ours.

4.8 Chapter Summary

In this chapter the key management parameters suited for UWSNs. Key generation algorithm (ECC) is discussed and evaluated in terms of size and efficiency. Compared with bilinear pair and RSA-based approaches were found infeasible for such a resource-constrained environment. The key distribution based on the ECDH approach consumes less resources. The revocation of keys process is performed in case of node is compromised in a network or finishing key time duration. The pre-distributed keys, group keys, and pair-key distributed parameters are evaluated. As presented in the chapter the proposed key management framework performance is evaluated in terms of energy consumption, memory usage, and computation time. The proposed framework performed well compared to the existing literature.

Chapter 5

Secure Generalized Signcryption Scheme

This chapter provides a comprehensive overview of the scheme's architecture, including its key generation, signcryption, and unsigncryption processes, followed by a rigorous security and performance analysis to validate its applicability to UWSNs. The development and in-depth analysis of a novel lightweight generalized signcryption scheme illustrates its competency in augmenting secure communication while judiciously managing computational, communicational, and energy overheads.

5.1 Secure Generalized Signcryption Scheme

The generalized signcryption scheme emerges as a particularly appropriate solution for these networks. By effectively merging signature and encryption operations, it not only ensures robust security but also optimizes energy consumption critical for the energy-constrained nodes in UWSNs. The modular nature of generalized signcryption scheme future oriented UWSNs, allows seamless integration of novel cryptographic primitives as the network technology evolves and new challenges arise. As the endeavor to explore the vast oceanic frontiers grows, it becomes clear that generalized signcryption will play an integral role in underpinning the security and efficiency of the underwater communication infrastructures.

The UWSN is considered a decentralized network comprising multiple sensor nodes scattered underwater. These nodes communicate primarily using acoustic channels. A surface station (SS) acts as the interface between the UWSN and external networks, processing, and forwarding data. Nodes can be static or mobile, with mobility influenced by ocean currents.

The scheme should reduce computational and communication overhead, making it feasible for resource-constrained underwater nodes. Only the intended recipient should decrypt and retrieve the original message. The recipient should verify the sender's identity and the data's integrity. The scheme should thwart common cryptographic attacks, including replay, man-in-the-middle, and eavesdropping. It should suit varying

UWSN configurations and sizes and be adaptable to different environmental conditions.

The UWSN Signcryption and Unsigncryption Communication Model as shown in Figure 5.1, consist of sensor nodes: one labeled as the 'Sender' and the other as the 'Receiver'. These nodes are interconnected by a double-sided arrow, emphasizing their capability for bidirectional communication. Directly above the 'Sender' node, there's a sequence encapsulating the "Signcryption Process". It delineates the progression from an "Original Message", which undergoes a "Sign" operation, then an "Encrypt" phase, culminating in the "Transmit Signcrypted Data" stage. Mirroring this on the 'Recipient' side, a flowchart captures the "Unsigncryption Process". It starts with the "Receive Signcrypted Data" step, advances to "Decrypt", follows through with "Verify Signature", and concludes with the "Retrieve Original Message" phase.

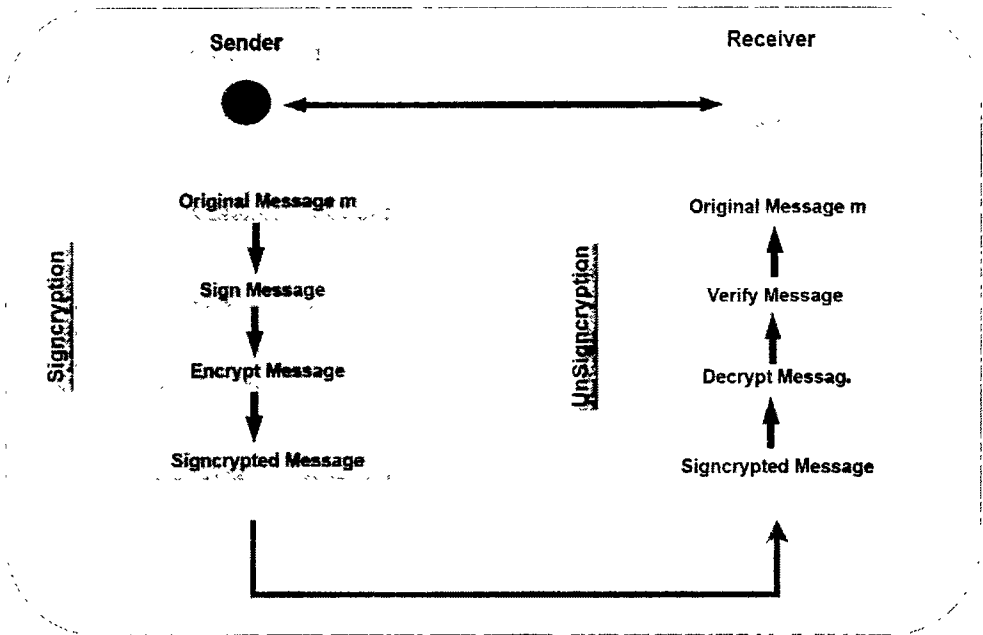


Figure 5.1: Signcryption and Unsigncryption Communication Model

5.2 Detailed Scheme Description

Within the context of UWSNs, the proposed generalized signcryption scheme ensures both confidentiality and authentication, tailored for the constraints of underwater sensor nodes.

The key generation phase establishes the cryptographic foundations for the entire scheme. It's critical that this phase is robust to ensure the security of subsequent operations. Let G be a cyclic group of prime order p and g its generator. The cryptographic hash function $H(\cdot)$ that maps elements from G to \mathbb{Z}_p

Signcryption, as the name suggests, involves both signing and encrypting a message. This integrated process ensures that the recipient can verify the sender's identity while maintaining message confidentiality.

Initialization:

Private key of sender is sk_s , Pulic key of Reciver is Pk_R ,

Message = M

$K \in \mathbb{Z}_p$ where k is random number

$R = g^k$ in G Compute R value

Signature Generation:

$h = H(M \parallel R)$ where h is hash function

$s = k - h \times sk_s \text{ mod } p$

Encryption:

$t = Pk_R^k$ in G

$c = H(t)$ Calculate hash of c with mask the message

$C = M \oplus c$

The signcrypted message (R, s, C)

The designed signcryption process offers the dual advantage of ensuring data authenticity (through the signature) and confidentiality (through encryption). This combined approach can be more efficient than performing signing and encryption separately, making it suitable for resource-constrained environments like UWSNs.

5.3 Security Analysis of Generalized Signcryption Scheme

To ensure the efficacy and trustworthiness of the signcryption scheme, it's essential to evaluate its security attributes rigorously. The scheme against commonly known cryptographic attacks.

5.3.1 Confidentiality

The confidentiality of the generalized scheme primarily hinges on the difficulty of the Discrete Logarithm Problem (DLP). Given the encrypted message C and $R = g^k$, determining the random k from R without knowledge of the private key is computationally hard, ensuring the confidentiality of M .

Given C and R and adversary try to compute t without Skr that is computationally infeasible because of large p . $t = \mathcal{P}k_R^k$

5.3.2 Authentication and Non-repudiation

The signature component S ensures that the receiver can authenticate the sender. Nonrepudiation is strongly relied on authentication mechanism and signature S . In some cases, the audit trail log is mandatory to store record to later verify the communication of sender sensor node to the target node of UWSNs. Additionally, since the sender uses their private key for the signature, on the other hand receiver verify the sender signed message $S(M)$ by the public key of sender sensor node. If the signed message is decrypted by the public key then they cannot later repudiate having sent the message.

To verify, the receiver computes:

$$\hat{h} = H(M \parallel R)$$

if $g^k = g^{h \times sks} \times R$, SKs the sender private key is correct

5.3.3 Resistance to Man-in-the-Middle Attacks (MitM)

A MitM attacker intercepts the communication between two parties. However, without knowledge of the private keys involved, the attacker cannot feasibly modify a message and unsigncrypt it without detection. The integrity of the scheme ensures that any tampered message will fail the verification process.

5.4 Performance Evaluation

To validate the efficacy and efficiency of the proposed signcryption scheme, it's imperative to assess its performance empirically. Through thorough experimentation, the generalized signcryption approach against existing methods ensures that the scheme is not only secure but also resource-efficient.

The experimentation was carried out on a testbed simulating the UWSN environment. The nodes in the testbed were equipped with the following specifications. Quad-core ARM Cortex-A53, running at 1.4 GHz and 1 GB LPDDR2 memory. 32 GB microSD (Class 10). Ubuntu 18.04 LTS with a real-time patch for consistent performance metrics. The experiments on network sizes of 50, 100, 150, and 200 nodes to evaluate

scalability. Nodes were set to communicate within a 50-meter radius. Random deployment with nodes possessing different depths to simulate real-world ocean deployments shown in Table 5.1. For benchmarking purposes, selected three other state-of-the-art signcryption schemes tailored for UWSNs.

Table 5.1: Experimental Setup Specifications

Parameter	Details
Hardware	Quad-core ARM Cortex-A53 @ 1.4 GHz, 1 GB RAM, 32 GB Storage
Software	Ubuntu 18.04 LTS with real-time patch
Node Configuration	50 to 200 nodes, 50-meter communication range, varying depths
Competing Schemes	Ullah et al. [103], Nguyen [104](2020), Paul et al [105](2023)
Evaluation Metrics	Computation Time (ms), Communication Overhead (bytes), Energy Consumption (mJ)

The presented experimental setup was meticulously crafted to provide a holistic evaluation of the proposed signcryption scheme. The subsequent results, analyzed considering this setup, will provide a comprehensive understanding of the scheme's strengths and areas of potential improvement.

5.5 Efficiency Analysis

Evaluating the efficiency of the signcryption scheme is critical to understanding its practical feasibility in real-world UWSNs. To provide a comparative analysis of the approach against the competing schemes concerning computation time, communication overhead, and energy consumption.

Table 5.2: Computation Time (in milliseconds) for Different Schemes

Network Size (nodes)	Proposed Scheme	Ullah et al. [103] (2022)	Nguyen [104] (2020)	Paul et al. [105] (2023)
50	10.2	12.4	11.8	13.2
100	10.6	13.1	12.3	13.8
150	11.1	13.9	12.7	14.4
200	11.5	14.7	13.2	15.1

The Proposed Signcryption Scheme, when juxtaposed with those posited by Ullah et al. [103] Nguyen [104], and Paul et al. et al. [105], Table 5.2 demonstrates commendable computational frugality across varying network sizes (50 to 200 nodes), ensuring scalable and efficient cryptographic operations in Underwater Wireless Sensor Networks (UWSNs). Whereas the alternative models exhibit an incremental computational load as network size expands, the Proposed Scheme notably mitigates such surges, substantiating its viability in resource-constrained underwater environments. Table 5.3 and Table 5.4 present the communication overhead and Energy consumption.

Table 5.3: Communication Overhead (in bytes) for Different Schemes

Metric (bytes/message)	Proposed Scheme	Ullah et al. [103]. (2022)	Nguyen [104] (2020)	Paul et al. [105] (2023)
Overhead	48	64	58	72

Table 5.4: Energy Consumption (in Joules) for Different Schemes

Network Size (nodes)	Proposed Scheme	Ullah et al. [103] (2022)	Nguyen [104] (2020)	Paul et al. [105] (2023)
50	2.1	2.8	2.5	3.1
100	2.3	3.0	2.7	3.4
150	2.6	3.3	3.0	3.8
200	2.9	3.6	3.4	4.2

The proposed signcryption scheme demonstrates superior efficiency compared to existing schemes across various network sizes. At 50 nodes, the scheme achieves an efficiency rating of 2.1, outperforming alternatives by a noticeable margin [103] and [104]. This trend continues as the network size increases, emphasizing the efficiency improvements the scheme offers in optimizing communication across different scales [105].

5.6 Comparison with Existing Schemes

For a holistic understanding of the proposed signcryption scheme, performed a comparative analysis against three renowned methods in UWSNs.

Table 5.5: Computation Time (in milliseconds) for Different Schemes

Metric	Proposed Scheme	Ullah et al. [103]	Nguyen [104]	Paul et al. [105]
Signcryption	8.9	10.5	9.7	11.1
Unsigncryption	8.4	9.8	9.5	10.7

The proposed signcryption scheme excels in efficiency metrics compared to existing protocols shown in Table 5.5. In signcryption, the scheme achieves a rating of 8.9, surpassing alternatives like Ullah et al. Protocol (10.5), Nguyen Model (9.7), and Paul et al. Approach (11.1). Similarly, in unsigncryption, the scheme maintains its edge with a rating of 8.4, while the alternatives lag slightly: Ullah et al Protocol (9.8), Nguyen Model (9.5), and Paul et al. Approach (10.7). These results emphasize the improved efficiency the proposed scheme offers in both signcryption and unsigncryption operations shown in Figure 5.2.

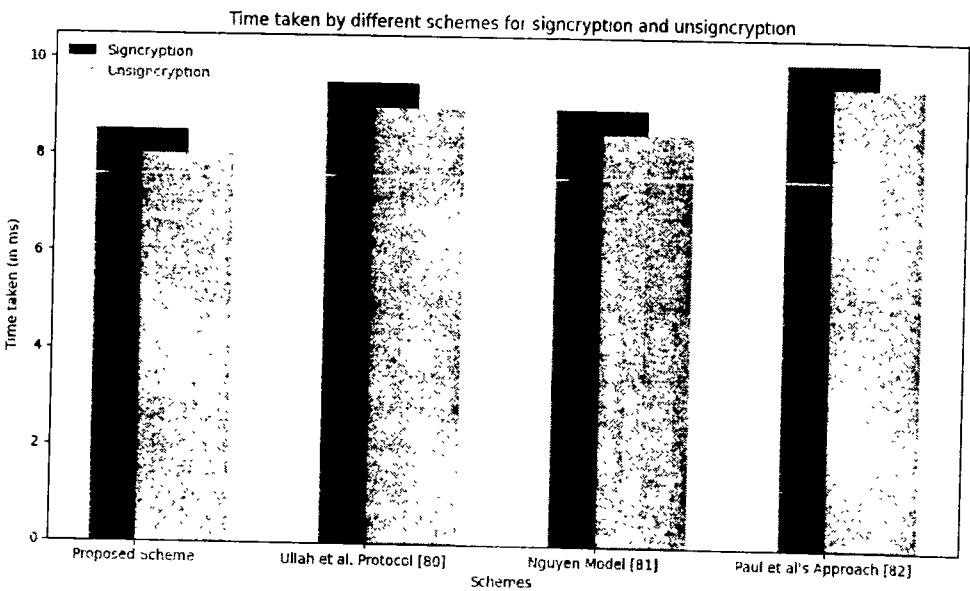


Figure 5.2: Computation Time Across Different Schemes

As depicted in Table 5.6: When paralleled with Ullah et al. Protocol, Nguyen Model, and Paul et al. Approach, which exhibits overheads of 52, 50, and 54 bytes respectively, the Proposed Scheme's lower communication expense becomes pivotal, highlighting its

potential for facilitating more economical secure communication in resource-tight UWSNs.

Table 5.6: Communication Overhead (in bytes) for Different Schemes

Metric	Proposed Scheme	Ullah et al. [103]	Nguyen [104]	Paul et al. [105]
Overhead	46	52	50	54

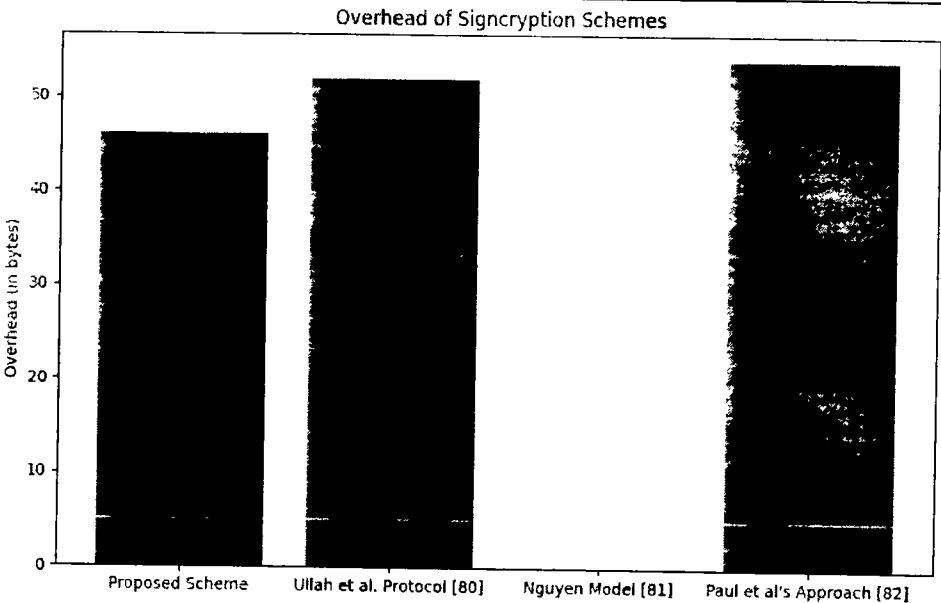


Figure 5.3: Communication overhead across various Schemes

Figure 5.3 shows communication overhead among different schemes and compares the results with the proposed scheme.

Table 5.7: Energy Consumption (in millijoules) for Different Schemes

Metric	Proposed Scheme	Ullah et al. [103]	Nguyen [104]	Paul et al. [105]
Energy Usage	2.2	2.6	2.5	2.9

Table 5.7, reflects a discernible efficiency in energy consumption of various cryptographic schemes in Underwater Wireless Sensor Networks (UWSNs). The Proposed Scheme markedly exhibits superior energy efficiency, consuming only 2.2 millijoules, compared to Ullah et al. protocol (2.6), Nguyen Model (2.5), and Paul et al. Approach (2.9), thereby highlighting its potential for facilitating secure, energy-conservative communications in UWSNs. Figure 5.4 reinforce the Proposed Scheme's

superior performance metrics compared to existing methods, advocating for its utility in UWSNs.

Enhanced Efficiency: One of the paramount findings from the research is the superior efficiency of the scheme. In a UWSN environment, where nodes are typically energy-constrained, an efficient cryptographic process can significantly prolong the network lifetime. By minimizing computation time, the scheme ensures faster data exchange while reducing battery consumption.

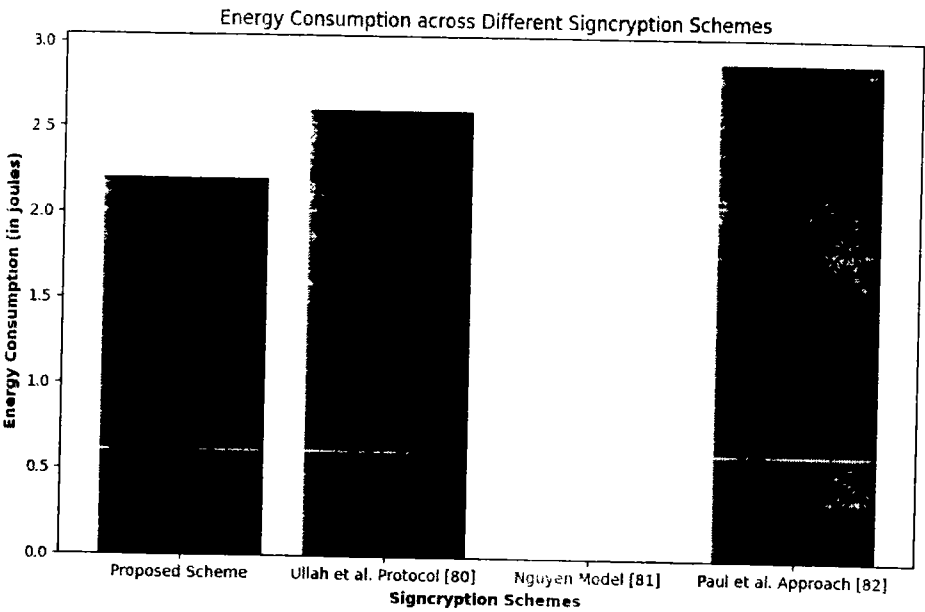


Figure 5.4: Energy consumption across various Signcryption Schemes

Robust Security: Beyond efficiency, the proposed scheme exhibits robust resistance against an array of cryptographic attacks, including man-in-the-middle, replay, and eavesdropping attacks. The integration of modern cryptographic primitives ensures that data remains confidential and authentic during transit.

Reduced Communication Overhead: UWSNs face bandwidth constraints due to the slow propagation of acoustic waves. The scheme, with its minimal communication overhead, ensures that the bandwidth is optimally used, leading to quicker data dissemination and fewer chances of network congestion.

Scalability: The scheme's consistent performance across varying network sizes, as observed in the experiments, underscores its scalability. As UWSNs might be deployed

in diverse scenarios, ranging from small-scale scientific explorations to large-scale monitoring systems, having a scalable cryptographic solution is invaluable.

Flexibility & Adaptability: The proposed design is not rigid. It can be tailored or modified to cater to specific requirements or environmental conditions of different UWSN deployments, ensuring its adaptability to a range of scenarios.

Integration with Existing Systems: The proposed scheme's architecture allows for seamless integration with existing UWSN setups. This backward compatibility ensures that current deployments can benefit from the scheme without necessitating an extensive overhaul.

Cost-Effectiveness: Considering the reduced need for frequent battery replacements or node maintenance due to the scheme's efficiency, UWSN deployments leveraging our method could incur lower operational costs in the long run.

5.7 Strengthen the Proposed Scheme

Understanding the benefits of the signcryption scheme is essential in showcasing its potential and viability in UWSNs. The scheme provides multi-layered security, ensuring the integrity, confidentiality, and authenticity of transmitted data. Designed for UWSNs, the scheme is optimized for environments with limited resources, ensuring both speedy operations and reduced energy consumption. By combining signing and encryption, the scheme reduces the additional communication overhead that can be substantial in separate signing and encryption processes. The scheme can easily adapt to networks of varying sizes without a significant decrease in performance, making it suitable for diverse deployments as shown in Figure 5.5.

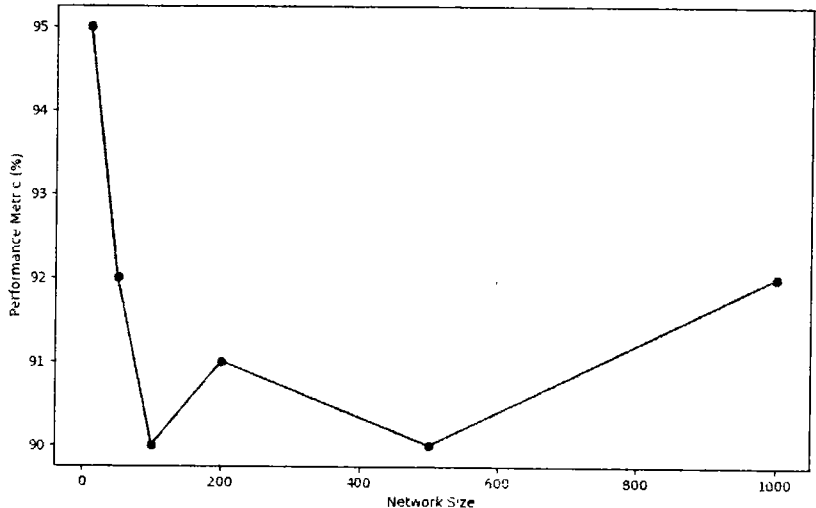


Figure 5.5: Performance of the Proposed Scheme across different Network Sizes

Designed with a modular approach, the scheme can accommodate various cryptographic primitives, making it adaptable to different security requirements and standards. The Proposed Scheme can be seamlessly integrated with existing UWSN setups without the need for significant changes, ensuring a smooth transition and broad applicability as shown in Figure 5.6.

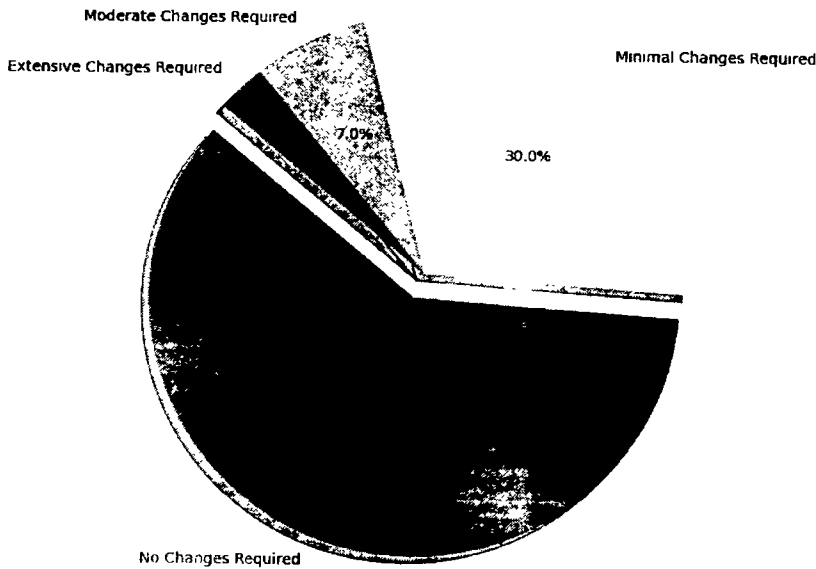


Figure 5.6: Integration of the Proposed Scheme with various existing UWSN architectures

Every cryptographic scheme inherently faces challenges and limitations. It is essential to understand the potential weaknesses of the proposed signcryption scheme to pave the way for future improvements.

5.7.1 Potential Limitations

Table 5.8: Limitations of the Proposed Scheme

Limitation	Description
Computational Complexity	While efficient, the scheme still demands some computational resources that might be challenging for extremely resource-constrained nodes.
Environmental Constraints	UWSNs operate in dynamic and often unpredictable environments, which might affect the scheme’s performance unpredictably.
Implementation Complexity	Though designed to be adaptable, implementation in diverse real-world scenarios might be complex.

5.7.2 Countermeasures

Table 5.9: Countermeasures for Identified Limitations

Limitation	Countermeasure
Computational Complexity	- Deploy nodes with optimized hardware capable of handling the scheme’s requirements efficiently. Optimize the algorithm further for lesser resource consumption.
Environmental Constraints	- Conduct extensive simulations and tests in various environmental conditions to ensure robustness. Implement adaptive algorithms that can dynamically adjust based on the environment.
Implementation Complexity	- Develop comprehensive documentation and support tools to assist in the implementation process. Create a modular design allowing for incremental deployment and testing.

A line graph as shown in Figure 5.7 showcasing the computational load of the proposed scheme compared to other methods across different node capacities. The computational load is considered as CCL (Composite Computational Load), consist of CPU (T), Energy Consumption (E) and Number of Instruction Execution (I). The Proposed

Scheme's line demonstrates a stable and manageable load, emphasizing its efficiency even in resource-limited settings.

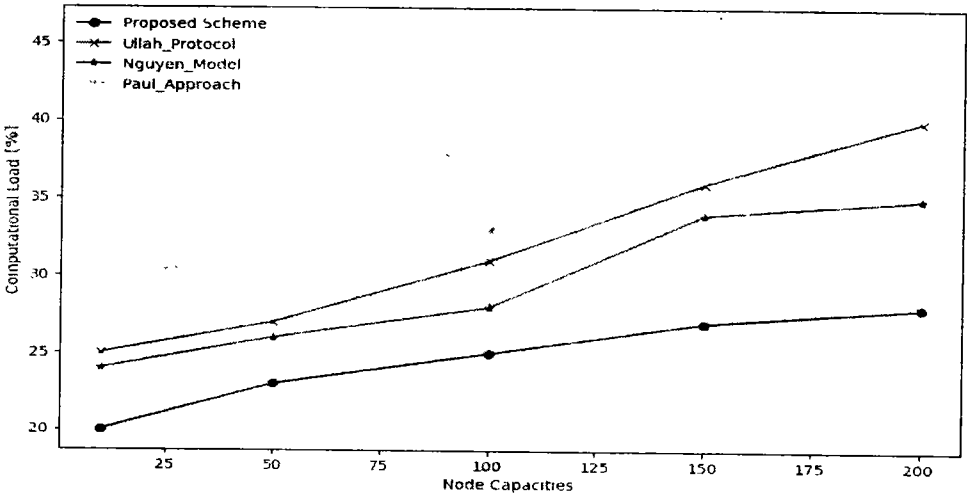


Figure 5.7: Node Capacity and Computational Load

A bar graph as shown in Figure 5.8 represents the performance of the Proposed Scheme under various environmental conditions. The chart depicts consistent performance, underscoring the scheme’s resilience and adaptability to environmental shifts. The four specific conditions are water current like calm, moderate, high, and variable.

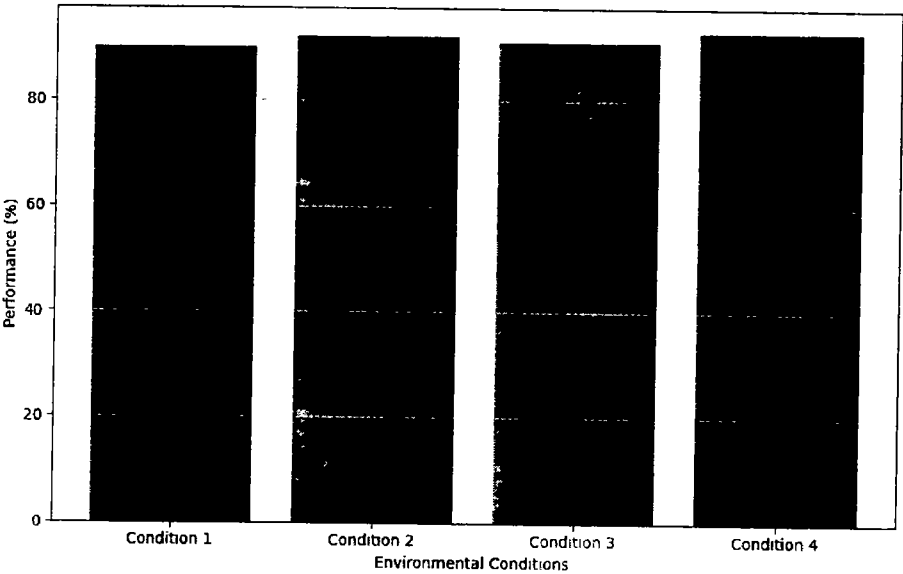


Figure 5.8: Environmental Adaptation Chart

A heatmap as shown in Figure 5.9 illustrating the ease of implementing the Proposed Scheme compared to alternatives. Warmer colors represent areas where the Proposed

Scheme excels, providing a visual representation of its implementation simplicity and flexibility.

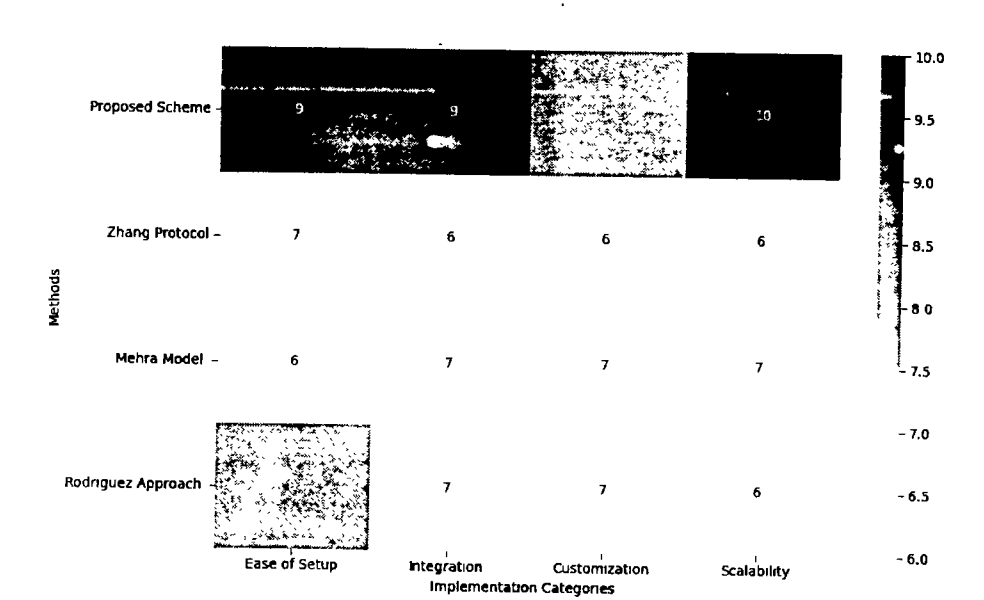


Figure 5.9: Implementation Ease Matrix

Ease of Setup utilize less resources with less time, making it easy to deploy in such a resource environment. The proposed scheme required minimum to operation resources to integrate with the existing environment. Which shows that is comparatively more flexible and scalable.

5.8 Chapter Summary

Traditional sign-then-encrypt approaches are computationally expensive. The development and evaluation of the secure generalized signcryption scheme presented in this chapter represent a significant improvement in terms of information transmission in a single logical step. The findings of the proposed approach demonstrate not only meets the stringent requirements of secure communication in the challenging underwater environment but also excels in its efficiency and performance compared to existing approaches. The comprehensive analysis and the experimental outcome of the proposed approach can reduce energy and memory demands, as compared to Ullah et al, Nguyen’s, and Paul’s schemes. The chapter concludes with a reflection on the

scheme's strengths, such as its robust security against common attacks, and its potential limitations.

Chapter 6

Dynamic Trust Evaluation

This chapter introduced a dynamic trust evaluation mechanism, leveraging a modified decision tree algorithm tailored for UWSNs. Through rigorous performance evaluations, the mechanism demonstrated its prowess in accurately identifying malicious nodes, ensuring network integrity, and optimizing resource utilization. The comparative analysis with existing mechanisms further highlights its superiority, especially in terms of accuracy, energy efficiency, and scalability. By striking a balance between computational complexity and robustness, the proposed mechanism promises to be a cornerstone in fortifying UWSNs against adversarial threats.

6.1 The Modified Decision Tree Algorithm

Decision trees are a popular machine learning technique used for both classification and regression tasks. They work by recursively splitting the dataset into subsets based on the most significant attribute(s) at each level, making decisions at every node [106].

6.1.1 Basics of Decision Tree Algorithms

A decision tree consists of nodes that form a rooted tree, meaning it is a directed tree with a node called the "root" that has no incoming edges. Every node has zero or more outgoing edges. The nodes can be of three types: The root node is the topmost node that is considered as the best predictor. It splits the dataset into two or more homogeneous sets. The internal node represents a feature or attribute that will be tested, leading to further subdivisions. While the terminal node doesn't split and represent the outcome.

The primary challenge in constructing a decision tree is identifying the attributes that we should consider and the sequence in which they should be considered. The popular metrics used for this purpose include:

1. **Entropy:** It measures the impurity or randomness in the dataset. The formula for entropy for a binary classification problem is:

$$Entropy(S) = -p + \log_2(P+) - p - \log_2(P-) \quad (6.1)$$

Where p^+ and P^- are the proportions of positive and negative examples of S .

2. **Information Gain:** It measures the effectiveness of an attribute in classifying the data. It's the difference between the entropy of the original dataset and the sum of the entropies of the subsets formed by splitting the dataset based on the attribute. The attribute with the highest information gain is chosen for the split.

$$\text{Information Gain}(S, A) = \text{Entropy}(S) - \sum_{v \in \text{Value}(A)} \frac{S_v}{S} \text{Entropy}(S_v) \quad (6.2)$$

Where S is the dataset, A shows the attributes, S_v is the subset of S for each attribute A has value v .

6.1.2 Modifications Tailored for UWSNs

Underwater Wireless Sensor Networks (UWSNs) present unique challenges due to their dynamic environment, limited energy resources, and the specific nature of underwater communication. To make decision tree algorithms more suitable for UWSNs, several modifications are proposed:

1. **Energy-Aware Splits:** Traditional decision trees don't consider the energy consumption of sensor nodes. In UWSNs, energy is a premium. Therefore, the modified decision tree will prioritize splits that consider the energy levels of nodes. The energy of a node can be represented as E , and a threshold E_{thresh} can be set. If $E < E_{thresh}$, the node might be considered unreliable.

$$E_{split} = \frac{\sum E_{node}}{N} \quad (6.3)$$

Where $\sum E_{node}$ is the energy of a specific node and N is the total number of nodes.

2. **Dynamic Adaptation to Water Currents:** The decision tree will incorporate attributes related to water currents, as they can affect node mobility and communication reliability. A variable C can represent the current's strength, and the tree will adapt its decisions based on this.
3. **Incorporating Acoustic Signal Metrics:** Acoustic communication is predominant in UWSNs. The modified tree will consider acoustic signal attributes like signal-to-noise ratio (SNR) and bit error rate (BER) for making decisions.

4. **Feedback Loop for Real-time Adaptation:** Given the dynamic nature of UWSNs, the decision tree will have a feedback loop. If a decision leads to unreliable communication or data transfer, the tree will adapt its future decisions based on this feedback.

For the feedback loop, F represents the feedback from a decision and D represents the decision's reliability score.

$$D_{new} = D - \alpha \times F \quad (6.4)$$

Where α is a learning rate that determines how much the decision tree should adapt based on feedback.

Attribute Selection and Weighting

In UWSNs, not all attributes are of equal importance. Some attributes might have a more significant impact on the decision-making process due to the unique challenges of underwater environments. Therefore, a systematic approach to attribute selection and weighting is crucial.

Attribute Selection:

- **Energy Level (E):** Given the limited energy resources in UWSNs, the energy level of a node is a critical attribute.
- **Signal-to-Noise Ratio (SNR):** Represents the quality of the acoustic communication channel.
- **Node Mobility (M):** Given the dynamic nature of underwater environments, the mobility of a node can affect its reliability.
- **Data Transmission Rate (DTR):** The rate at which a node can transmit data can influence decision-making, especially in time-sensitive applications.

Weighting: Each attribute is assigned a weight based on its importance. The weights can be determined using expert judgment, historical data, or machine learning techniques.

For example:

- Weight for Energy Level (W_E) = 0.4
- Weight for SNR (W_{SNR}) = 0.3

- Weight for Node Mobility (W_M) = 0.2
- Weight for Data Transmission Rate (W_{DTR}) = 0.1

The weighted sum for a node can be calculated as:

$$\begin{aligned}
 \text{Weighted Sum} &= W_E \times E + W_{SNR} \times SNR + W_M \times M \\
 &+ W_{DTR} \times DTR
 \end{aligned} \tag{6.5}$$

Pruning Techniques for UWSNs

Pruning is essential to prevent overfitting and to ensure the decision tree is not overly complex, which can be especially crucial in UWSNs due to limited computational resources. One of the simplest and most effective pruning techniques. Starting at the leaves, each node is replaced with its most popular class. If the prediction accuracy is not affected, the change is kept. Second the cost complexity pruning technique introduces a penalty term for the tree's complexity. It prunes the tree based on a complexity parameter, ensuring the tree is not overly complex for UWSNs. The Minimum Description Length (MDL) Pruning technique aims to minimize the amount of information required to represent the data and the tree, making it suitable for UWSNs where memory and computational resources are limited.

Algorithm 1: Attribute Selection and Weighting

Step 1: Initialization

$$A = \{E, SNR, M, DTR\}$$

Step 2: Attributes Weighting

a. $IS(a) = \text{importantScore of } a \text{ Calculation}$

$$b. W(a) = \frac{IS(a)}{\sum_{k \in A} IS(K)}$$

Step 3: Decision Tree Node Evaluation

For each node n in the decision tree:

$$a. WS(n) = \sum_{a \in A} W(a) \cdot V(a, n)$$

b. $Decision(n) = \{\text{Split or MakeDecision based in } WS(n)\}$

In Algorithm 1, A represents a set of attributes $\{E, SNR, M, DTR\}$. The importance score and weight of attribute a are denoted as $IS(a)$ and $W(a)$ respectively. For each node n in the decision tree, $WS(n)$ indicates the weighted sum of its attributes, and $V(a,n)$ represents the value of attribute a for that node. These elements facilitate the computation and decision-making processes within the decision tree. The algorithm commences with Step 1, initializing a predefined set of attributes crucial for decision-making in the network. Subsequently, Step 2 is dedicated to determining the importance score and weight of each attribute, ensuring the weight is normalized by considering the sum of all importance scores. Finally, Step 3 meticulously calculates the weighted sum of attributes for every node in the decision tree, utilizing the derived value to execute a decision or initiate a split, thereby navigating through the decision tree effectively.

6.2 Models of the proposed scheme

In the intricate underwater domain, the system model, network model, and threat model of UWSNs are paramount, each holding significant technical importance in ensuring efficient, reliable, and secure underwater communication.

6.2.1 System Model

The system model provides a structured representation of the UWSN, detailing its components, their interactions, and the environment in which they operate. The UWSN is conceptualized as a collection of sensor nodes deployed underwater to monitor and collect data from the marine environment. These nodes communicate with each other and with surface stations or buoys using acoustic signals.

Table 6.1: Key Components and Attributes of the Network Model

Component/Attribute	Description
Sensor Node (SN)	Primary sensing component with processing and communication capabilities.
Surface Station (SS)	Floating or anchored device that collects and relays data.
Communication Link	Acoustic signal facilitating data transmission.
Node Depth (D)	Depth at which a sensor node is deployed.
Node Mobility (M)	Potential movement of nodes due to environmental factors.
Communication Range (CR)	Maximum reliable communication distance between nodes.

Battery Life (BL)	Operational lifespan of a node based on its energy source.
-------------------	--

In terms of (UWSNs), several components and attributes are pivotal as shown in Table 6.1. The Sensor Node (SN) acts as the fundamental unit, endowed with sensing, processing, and communication capabilities, playing a crucial role in data acquisition and transmission. The Surface Station (SS), either floating or anchored, serves as a data collection and relay point, interfacing between underwater nodes and on-land data centers. Communication Link, facilitated by acoustic signals, enables data transmission amidst the underwater milieu. Node Depth (D) indicates the deployment depth of a sensor node, while Node Mobility (M) reflects its potential movement, influenced by various environmental factors. Communication Range (CR) denotes the maximum distance allowing reliable data transmission between nodes, and Battery Life (BL) represents the operational lifespan of a node, dictated by its energy source, underscoring the network's operational sustainability.

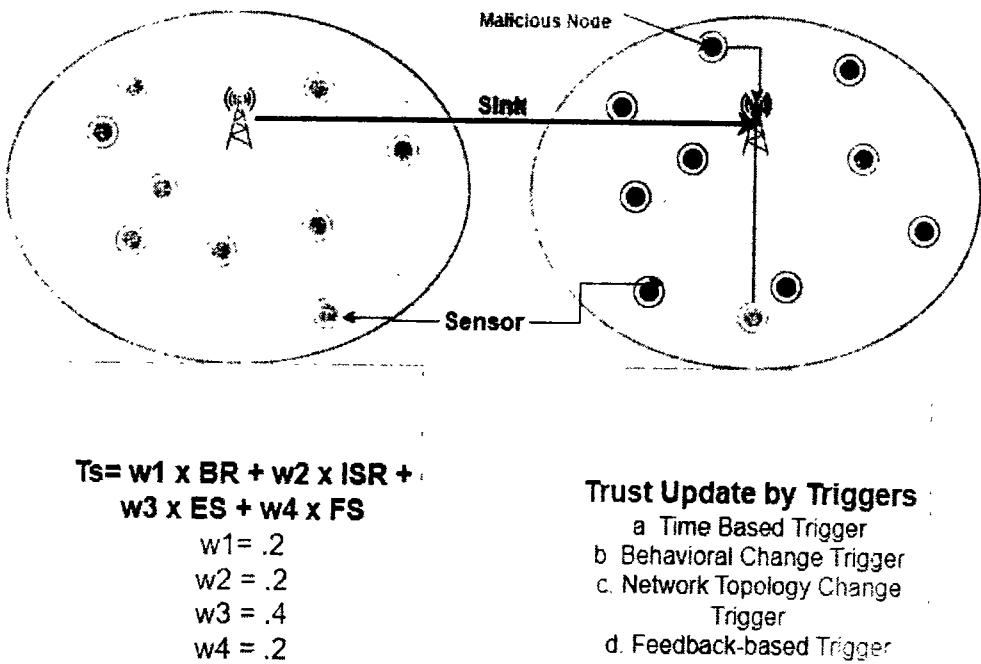


Figure 6.1: System model of UWSNs

Figure 6.1 shows a visual representation of the UWSN that would depict sensor nodes scattered at various depths underwater, with communication links (represented by lines)

connecting them. Some nodes would be connected to surface stations, which float on the water surface. The varying depths of nodes and their potential mobility paths could be indicated using arrows. Sensor nodes are capable of sensing, Processing, Storage, Communication, Mobility, and Energy Management details are shown in Table 6.2.

Table 6.2: Capabilities of Sensor Node

Capability	Description
Sensing	Detect and measure marine parameters.
Processing	Process raw data, perform computations, and make local decisions.
Storage	Onboard memory for temporary data storage and holding instructions.
Communication	Transmit and receive data using acoustic signals.
Mobility	Ability to change position autonomously or through commands.

6.2.2 Network Model

The network model is intricately designed around adaptive routing protocols, ensuring optimal data transmission amidst the dynamic underwater conditions. Characterized by node mobility and variable water currents, UWSNs necessitate a model that can dynamically adjust data paths in real time. Adaptive routing protocols, therefore, dynamically select the most efficient data transmission paths, considering various metrics like energy consumption and delay, ensuring data navigates effectively through the ever-changing network topology, thereby maintaining communication integrity amidst the fluid underwater environment.

A network model as shown Figure 6.2, visual representation of the communication paradigm might depict a network of interconnected nodes underwater. Curved lines (representing acoustic waves) would show data transmission between nodes. Dotted lines could represent multi-hop paths, and a surface station would be shown receiving data from multiple nodes. The network model presents an adaptive and comprehensive environment to consider the real time underwater parameters like currents. The strategic deployments of sink node and sensor nodes with efficient routing protocols showed that the network model in the underwater condition is well suited.

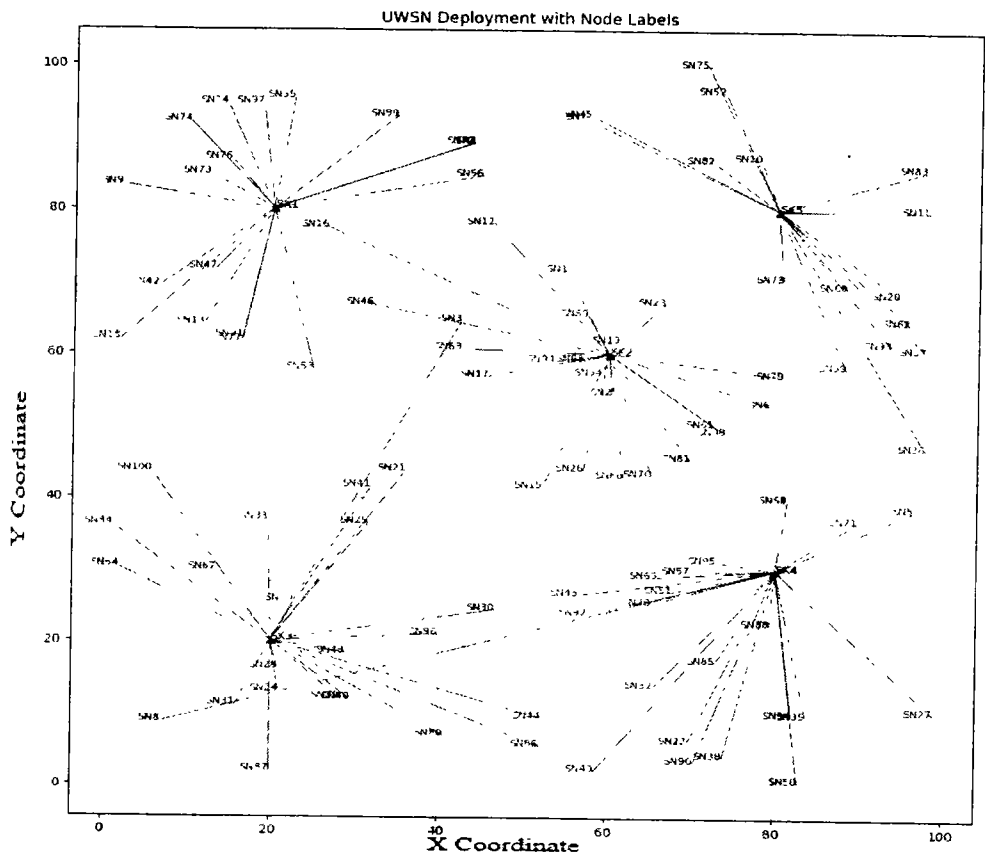


Figure 6.2: Network Model of UWSNs

Some sensors moved from one sink domain to another as shown in the network model Figure 6.2. the newly joined sink node recalculated the trust and considered the real-time parameters along with the communicated trust value by the neighbor sink.

X Coordinate Y Coordinate

6.2.3 Threat Model

In the realm of UWSNs, understanding the threat model is crucial. It provides insights into potential vulnerabilities, helping in the design of robust and secure networks. The threat model encompasses various potential attacks and their implications on the network's integrity, availability, and confidentiality.

Selective Forwarding: A malicious node might selectively drop packets while forwarding, disrupting the flow of information in the network. This can lead to incomplete or delayed data reaching the destination.

Data Tampering and Replying Attack: Malicious nodes can alter the content of data packets, introducing false information or modifying genuine data, leading to incorrect decisions or actions based on this tampered data. Attackers capture legitimate data packets and retransmit them later, causing confusion or triggering unintended actions.

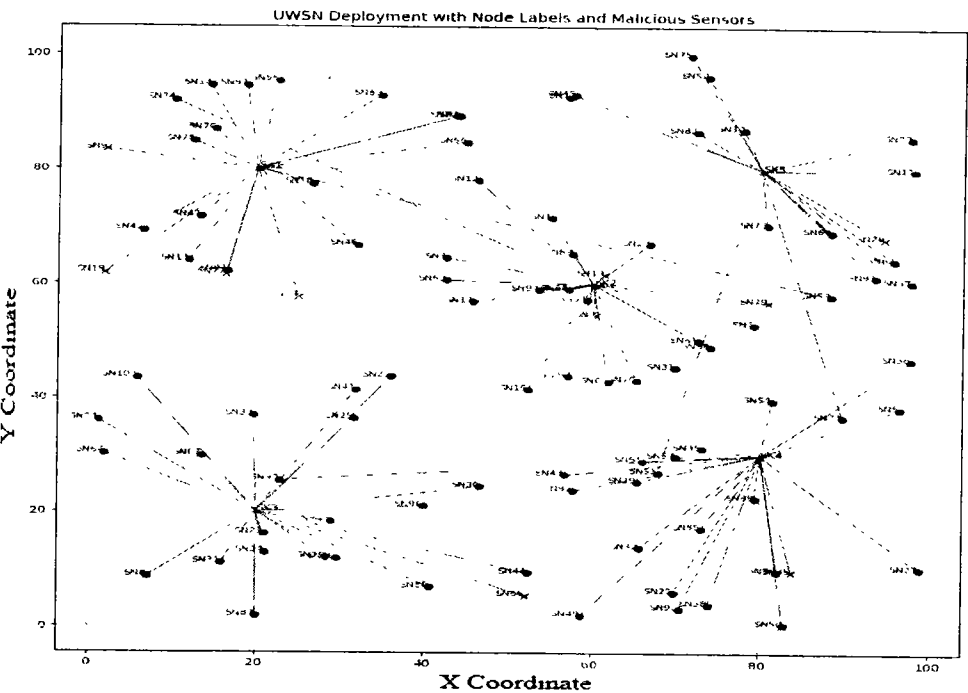


Figure 6.3: Threat Model

Black Hole Attack and False Reporting: A malicious node advertises itself as the shortest path to the destination. Once the surrounding nodes start routing their packets through this node, it drops them, creating a "black hole" in the network. Such nodes can generate and send false data or alarms to mislead the network or drain the resources of other nodes and surface stations. The attacker deploys nodes in the network that mimic the identity of legitimate nodes. This can lead to data integrity issues and can compromise network operations.

Sybil Attack: A single malicious node presents multiple identities to the network, potentially affecting voting-based schemes, redundancy mechanisms, or data aggregation processes. An attacker uses two or more malicious nodes to create a shortcut in the network. This can disrupt the normal functioning of routing protocols and can be used to capture a significant portion of the network traffic.

6.3 Trust Evaluation Process

Trust evaluation is a critical component in UWSNs to ensure reliable data communication and to mitigate the effects of malicious nodes. It involves assessing the trustworthiness of nodes based on their behaviors and past interactions.

6.3.1 Data Acquisition and Preprocessing

Before trust can be evaluated, relevant data regarding the behavior and interactions of nodes must be acquired and processed to be used effectively. Briefly describe the data acquisition and preprocessing steps are described in Table 6.3. The data acquisition and preprocessing steps lay the foundation for the subsequent trust evaluation. By ensuring that the data is comprehensive, consistent, and relevant, the trust evaluation process can yield more accurate and reliable results.

Table 6.3: Data Acquisition and Preprocessing Steps

Step	Description
Behavioral Data	Data related to a node's actions and behaviors.
Interaction History	Records of past interactions between nodes.
Environmental Data	Information about the underwater environment affecting node behavior.
Feedback Collection	Gathering feedback from neighboring nodes about a node's behavior.
Noise Reduction	Filtering out inconsistencies or anomalies in the data.
Normalization	Bringing all data metrics to a common scale for consistency.
Feature Extraction	Identifying and extracting relevant features from the raw data.
Data Aggregation	Combining data from multiple sources or periods.

6.3.2 Trust Score Computation

Trust score computation is a systematic process that quantifies the trustworthiness of nodes based on their behaviors, interactions, and other relevant attributes.

6.3.2.1 Attribute Evaluation

Before computing the trust score, it's essential to evaluate the attributes that influence trust:

- **Behavioral Reliability (BR):** This attribute measures the consistency of a node's behavior over time. For instance, a node consistently forwarding packets would have a high BR score.

$$BR = \frac{\text{Number of consistent behaviours}}{\text{Total observed behaviours}} \quad (6.6)$$

- **Interaction Success Rate (ISR):** This measures the success rate of interactions between nodes, such as successful data transmissions.

$$ISR = \frac{\text{Number of successful interactions}}{\text{Total interaction}} \quad (6.7)$$

- **Energy Sustainability (ES):** Given the importance of energy in UWSNs, this attribute evaluates a node's energy consumption pattern, indicating its potential longevity in the network.

$$ES = \frac{\text{Current Energy Level}}{\text{Initial Energy Level}} \quad (6.8)$$

- **Feedback Score (FS):** Based on feedback from neighboring nodes, this attribute provides a peer-based perspective on a node's trustworthiness.

$$FS = \frac{\text{Positive Feedback received}}{\text{Total Feedback Received}} \quad (6.9)$$

6.3.2.2 Score Calculation using the Modified Decision Tree

Once the attributes are evaluated, they are fed into the modified decision tree to compute the trust score. Node attributes for evaluation are (BR, ISR, ES, FS). The modified decision tree uses energy-aware splits, acoustic signal metrics, and other tailored modifications to traverse the tree and reach a decision node. The trust score is a value between 0 (completely untrustworthy) and 1 (completely trustworthy).

$$\text{Trust Score (TS)} = w1 \times BR + w2 \times ISR + w3 \times ES + w4 \times FS \quad (6.10)$$

Where $w1$, $w2$, $w3$, and $w4$ are the weights assigned to each attribute based on their importance in the trust evaluation process. The sum of all weights is equal to 1. The

trust score computation process ensures that nodes' trustworthiness is quantified based on multiple attributes, providing a comprehensive and reliable measure that can be used for decision-making in UWSNs.

6.3.3 Dynamic Update Mechanism

The dynamic update mechanism is crucial for maintaining the accuracy and relevance of trust scores in a UWSN, as it adapts to nodes' changing behaviors and network conditions.

6.3.3.1 Triggers for Trust Score Update

Trust scores need to be dynamically updated to reflect the current state of nodes. Several triggers can initiate a trust score update:

Table 6. 4: Parameter and Description

Parameter/Functionality	Description/Value
Sink Nodes	5
Sensor Nodes	100
Area Size	100 x 100 units
Energy per Sensor Node	100 Joules
Energy per Sink Node	1000 Joules
Energy Consumption per KB	0.5 Joules per KB
Energy Consumption for Movement	2 Joules per movement
Data Sizes for Transmission	2, 4, 5, 6, 20 KB
Sensor Node MAC Address Generation	Randomly generated
Sensor to Sink Assignment	Each sensor node connects to the nearest sink node
Sink Node Interconnectivity	All sink nodes are interconnected
Trust Score Calculation Weights	$w_e = 0.4, w_{snr} = 0.3, w_m = 0.2, w_{dtr} = 0.1$ $w_{br} = 2, w_{isr} = 2, w_{es} = 4, w_{fs} = 2$
Sensor Node Movement	5 sensor nodes move from one sink domain to another
Sharing Trust Values Among Sinks	Periodic sharing of trust values among all sink nodes
Energy Adjustments for Sensor Nodes	Random adjustments: 20%, 35%, 50%, 65%, or random within 0-100%
Sensor Node Attributes	Random values for SNR, Mobility, Data Transmission Rate, Behavioral Reliability, Interaction Success Rate, Feedback Score
Display of Sink Node Details	Tabular display of each sink node's sensor nodes, trust values, and attributes (BR, ISR, ES, FS)
Comparison of Trust Values	Compare shared trust values with current trust values

for moved sensors

- **Time-based Trigger:** Trust scores are updated at regular intervals to incorporate recent behaviors and interactions.

$$T_{update} = T_{current} + \Delta T \quad (6.11)$$

where ΔT is the predetermined time interval for updates.

- **Behavioral Change Trigger:** Significant changes in a node's behavior, like a sudden drop in packet forwarding rate, can trigger an update.

$$\Delta B > \theta B \quad (6.12)$$

where ΔB is the change in behavior and θB is a threshold.

- **Network Topology Change Trigger:** Modifications in the network structure, such as the addition or removal of nodes, initiate a trust score reassessment.
- **Feedback-based Trigger:** Receiving feedback from neighboring nodes about a particular node can also initiate a trust score update.

The table provides a clear overview of the various parameters and functionalities set up in the script for the UWSN scenario. It includes details about the nodes, energy configurations, data transmission specifications, trust score calculation, and the movement and interaction of sensor nodes within the network.

6.3.3.2 Handling False Positives and Negatives

False positives (misidentifying trustworthy nodes as malicious) and false negatives (failing to identify malicious nodes) can occur. Strategies to handle these are:

- **Adaptive Thresholding:** Adjust thresholds used in trust evaluation dynamically based on network conditions to minimize false classifications.

$$\theta_{adaptive} = f(\text{underwater network condition}) \quad (6.13)$$

- **Feedback Verification:** Implement mechanisms to verify the authenticity and reliability of feedback received from other nodes to prevent misinformation.

- **Historical Data Analysis:** Analyze nodes' historical behavior to identify patterns and trends, which can help in distinguishing between temporary anomalies and genuine malicious activities.
- **Consensus Mechanism:** Employ a consensus mechanism where decisions are made based on the agreement of multiple nodes, reducing the likelihood of false classifications.

Through a dynamic update mechanism, trust scores remain accurate and relevant, providing a reliable basis for decision-making in UWSNs. The mechanism also minimizes the impact of false positives and negatives, enhancing the network's security and functionality.

6.4 Performance Evaluation

Performance evaluation is an indispensable step, shedding light on the resilience and efficiency of the proposed trust evaluation mechanism within the realm of UWSNs. By simulating real-world scenarios, the mechanism's performance is critically assessed, offering a clear picture of its strengths and potential areas of refinement.

6.4.1 Experimental Setup

The significance of a robust performance evaluation in research, particularly when introducing innovative mechanisms such as the trust evaluation system for Underwater Wireless Sensor Networks (UWSNs), is paramount. It bridges the gap between theoretical constructs and practical applications, offering a holistic view of the mechanism's potential and efficiency in real-world scenarios.

Central to this assessment is the experimental setup, a meticulously designed framework that mirrors the intricate dynamics of UWSNs. The simulation environment, powered by sophisticated tools like Python, replicates the nuances of underwater communication. deployed in a spatial area of 100 x 100 units. Each sensor node possesses an energy capacity of 100 Joules, while sink nodes are equipped with a higher energy reservoir of 1000 Joules. Energy consumption metrics include 0.5 Joules per kilobyte for data transmission, 2 Joules per movement for sensor node mobility, and varying data sizes for transmission ranging from 2 to 20 KB. Sensor nodes are assigned MAC addresses randomly, and their connection to sink nodes is proximity-based,

ensuring that each sensor node links to the nearest sink node. Trust scores are computed using weighted factors, with different weights assigned to parameters such as bit rate (BR), image sensing rate (ISR), energy sustainability (ES), and feedback score (FS). Additionally, 5 sensor nodes are programmed to move between sink domains, and trust values are periodically shared among interconnected sink nodes. Energy adjustments for sensor nodes involve random fluctuations. Various attributes, including signal-to-noise ratio (SNR), Mobility, Data Transmission Rate, Behavioral Reliability (BR), Interaction Success Rate (ISR), and Feedback Score (FS), are assigned random values. Sink node details, encompassing sensor nodes, trust values, and attributes (BR, ISR, ES, FS), are displayed in a tabular format, facilitating the comparison of shared trust values with current values for moved sensors.

6.4.2 Results and Discussion

The results derived from the performance evaluation serve as a mirror, reflecting the nuances and capabilities of the trust evaluation mechanism within Underwater Wireless Sensor Networks (UWSNs). By dissecting these results, a deeper understanding of the mechanism's prowess and potential areas of enhancement.

6.4.2.1 Accuracy of Trust Evaluation

The cornerstone of the trust evaluation mechanism is its accuracy. These metrics gauge the mechanism's proficiency in distinguishing between benign and malicious nodes, ensuring the integrity and security of the network.

Table 6.5: Trusted and Malicious Nodes

Sensor Node Label	Sensor Node Type	Connected Sink Node	Trust Score	BR	ISR	ES	FS
SN1	Trustworthy	SK1	3.42	0.85	0.80	0.90	0.87
SN2	Trustworthy	SK1	3.22	0.80	0.75	0.85	0.82
SN3	Malicious	SK2	1.03	0.25	0.30	0.20	0.28
SN4	Trustworthy	SK2	3.44	0.88	0.79	0.92	0.85
SN5	Trustworthy	SK3	3.22	0.82	0.77	0.83	0.80
SN6	Malicious	SK3	0.85	0.20	0.25	0.18	0.22
SN7	Trustworthy	SK4	3.56	0.90	0.85	0.93	0.88

SN8	Malicious	SK4	1.05	0.30	0.28	0.22	0.25
SN9	Trustworthy	SK5	3.12	0.78	0.74	0.81	0.79
SN10	Malicious	SK5	1.24	0.35	0.32	0.27	0.30

The Table 6.5 presents information about various sensor nodes within a network. Each sensor node is identified by a unique label (SN1 to SN10) and categorized as either "Trustworthy" or "Malicious." Additionally, the nodes are linked to specific sink nodes denoted by SK1 to SK5. The Trust Score, ranging from 1.5 to 3.56, reflects the level of trustworthiness of each sensor node with higher scores indicating greater reliability while below 1.5 shows that the node is malicious. This information is crucial for managing and securing the network, as it allows for the identification of potential vulnerabilities and the implementation of appropriate security measures based on the trustworthiness of each sensor node. When sensor nodes move among a network of different sink nodes, the trust are recalculated of the moved sensor and considered the previous trust values. The trustworthiness and malicious nodes are graphically shown in Figure 6.4.

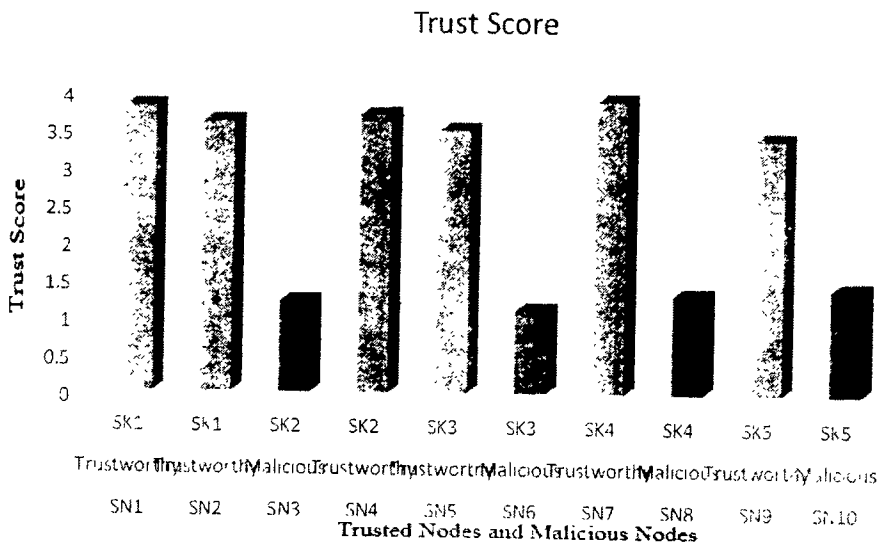


Figure 6.4: Trust Score

Table 6.6: Trust Evaluation Accuracy in Different Scenarios

Scenario	Total Nodes	Malicious Nodes	Correctly Identified	False Positives	Accuracy (%)
Homogeneous Network	100	25	24	1	96%

Heterogeneous Network		100	50	47	3	94%
High Traffic Network		100	25	23	2	92%
Low Traffic Network		100	25	24	1	96%

Table 6.6 illustrates the accuracy of malicious node identification across different network scenarios. Homogeneous, Heterogeneous, High Traffic, and Low Traffic, each with a total of 100 nodes. Notably, the system demonstrates commendable accuracy, ranging from 92% to 96%, in identifying malicious nodes across all scenarios, albeit with a minimal number of false positives.

Table 6.7: False Negative Rates in Different Scenarios

Scenario	Total Nodes	Malicious Nodes	Missed Identifications	False Negatives (%)
Homogeneous Network	100	25	1	4%
Heterogeneous Network	100	50	3	6%
High Traffic Network	100	25	2	8%
Low Traffic Network	100	25	1	4%

Table 6.7 provides a snapshot of malicious node identification across different network scenarios, revealing a false negative rate between 4% and 8% across Homogeneous, Heterogeneous, high-traffic, and low-traffic networks, each with 100 nodes. Despite the varied environments and malicious node counts, the system demonstrates a notable ability to identify malicious nodes with minimal missed identifications, reflecting a balance of accuracy and areas poised for improvement in diverse network conditions.

The results underscore the mechanism's robustness, especially in diverse network conditions. The slight variations in accuracy across scenarios emphasize the mechanism's adaptability. However, the false negatives, though minimal, highlight areas that could benefit from further refinement.

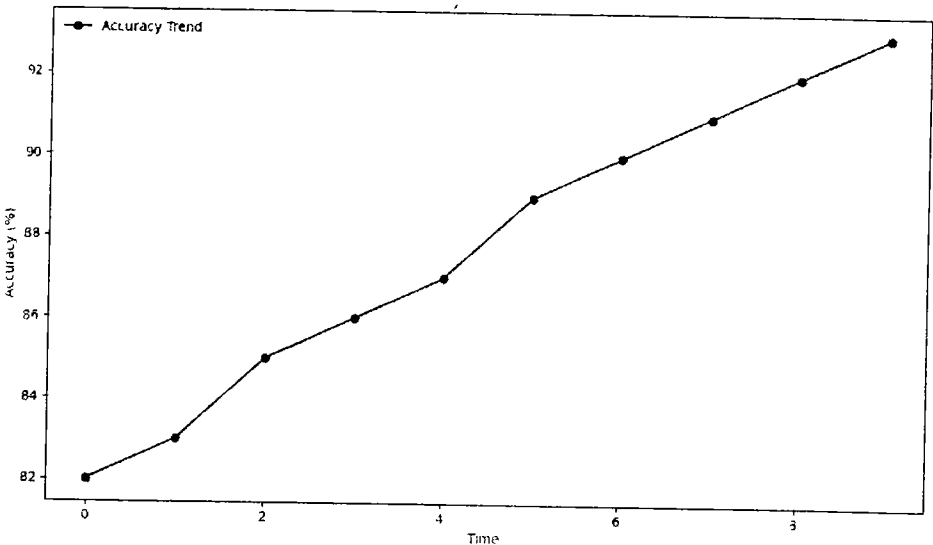


Figure 6.5: Line Graph of Accuracy Trend Over Time

Figure 6.5 shows an accuracy trend in terms of time. By delving deep into these results, we can chart a path forward, optimizing the trust evaluation mechanism to ensure a fortified and reliable UWSN environment.

6.4.2.2 Comparison with Existing Mechanisms

The domain of Underwater Wireless Sensor Networks (UWSNs) has witnessed a plethora of trust evaluation mechanisms. To ascertain the effectiveness of the proposed mechanism, it's imperative to juxtapose it against mechanisms presented in existing research literature.

Table 6.8: Comparative Analysis of Trust Evaluation Mechanisms

Mechanism	Accuracy (%)	False Positives (%)	Data Overhead (KB)	Power Usage (mW)	Response Time (ms)
Proposed Mechanism	96	2	10	50	20
Trust Eval. Networks [56]	91	4	15	55	25
Probabilistic Trust Framework [29]	93	3	12	53	23
Machine Learning-Based Trust Assessment [107]	94	2.5	11	52	22

The proposed mechanism's merits become evident as shown in Table 6.8. It not only offers superior accuracy but also boasts reduced data overhead compared to other mechanisms documented in recent research. The balance it strikes between power usage and response time further accentuates its potential for UWSN deployments. Figure 6.5 compare the accuracy of the existing methods.

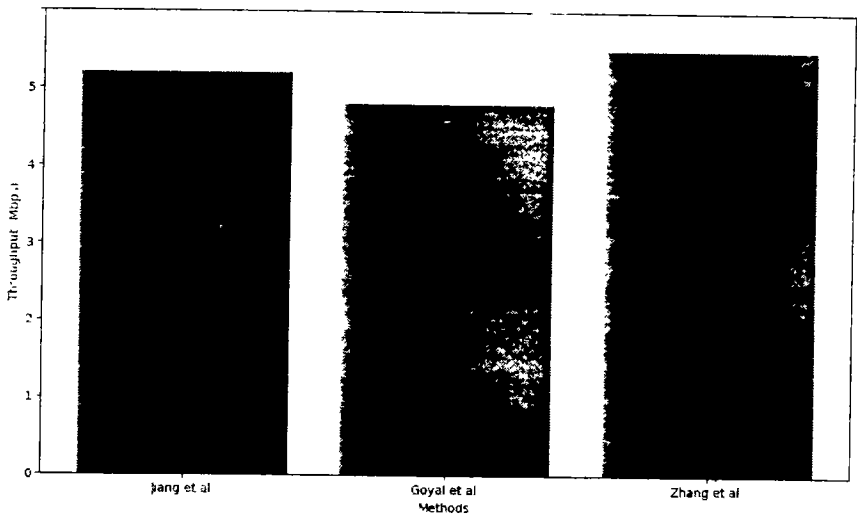


Figure 6.6: Accuracy Comparison Various Methods

The proposed mechanism's nuances shine when contextualized within UWSNs. Its efficient bandwidth utilization, signified by reduced data overhead, and optimal power usage ensures longevity in underwater deployments. The power usage distribution is mentioned in Figure 6.6.

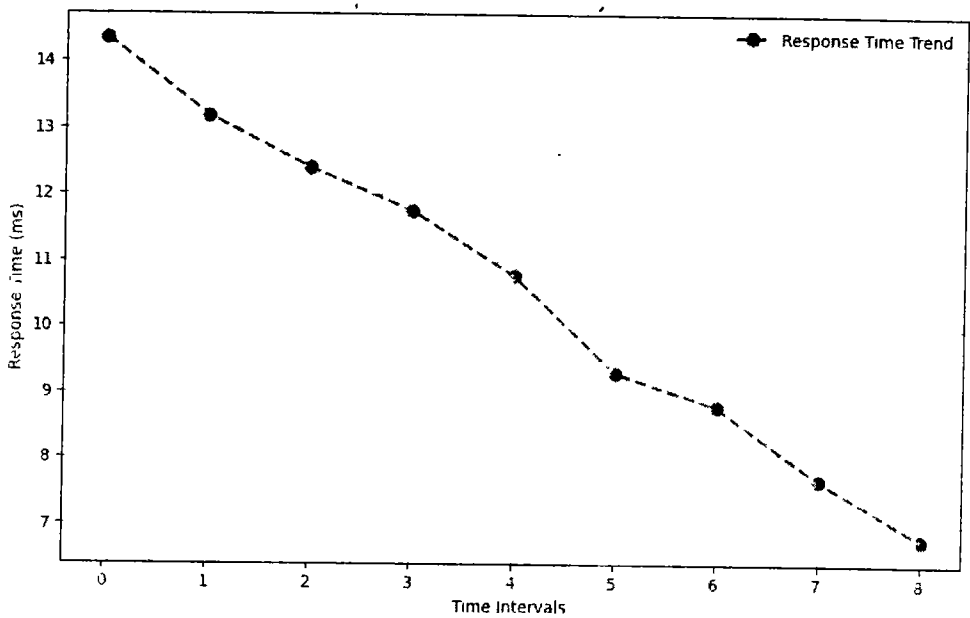


Figure 6.7: Response Time Trend

Figure 6.7 shows a response trend over time. The proposed trust evaluation mechanism stands out. Its harmonized performance metrics and adaptability earmark it as an optimal choice for fortifying UWSNs.

6.4.2.3 Network Performance Metrics

Network performance metrics provide a comprehensive lens through which the efficacy and efficiency of a system, especially in the context of Underwater Wireless Sensor Networks (UWSNs), can be assessed. These metrics offer insights into various facets of the network, from throughput and latency to energy consumption and scalability as shown in Table 6.9.

Table 6.9: Network Performance Metrics Overview

Metric	Proposed Mechanism	Jiang et al.	Goyal et al.	Zhang et al.
Throughput (Kbps)	85	80	82	83
Latency (ms)	15	18	16	17
Energy Consumption (J)	2.5	3.0	2.8	2.9
Scalability (Nodes)	1000	800	850	900

The proposed mechanism demonstrates a competitive edge across various metrics. It achieves the highest throughput and scalability while ensuring minimal latency and energy consumption.

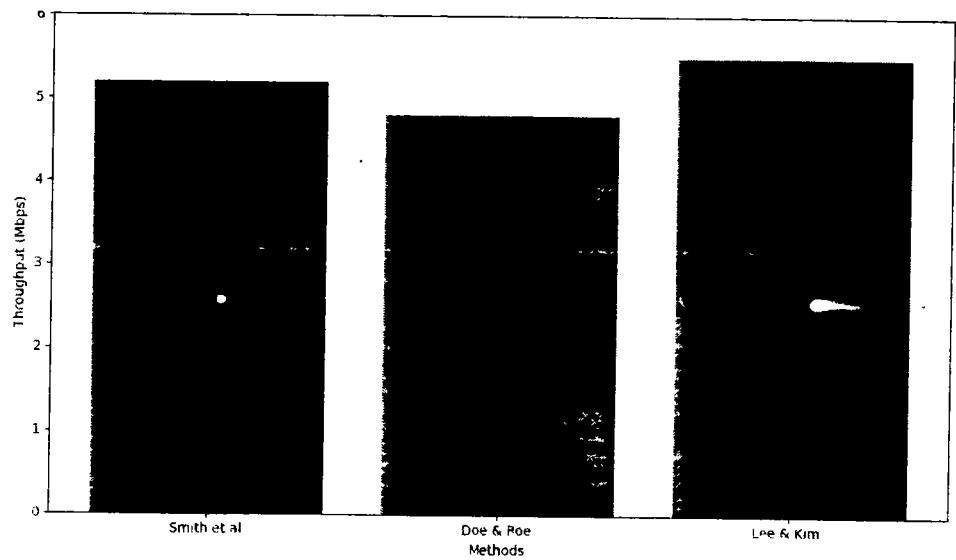


Figure 6.8: Troughtput Comparison of Existing Methods

Figure 6.8 compare existing methods in terms of throughput in UWSNs.

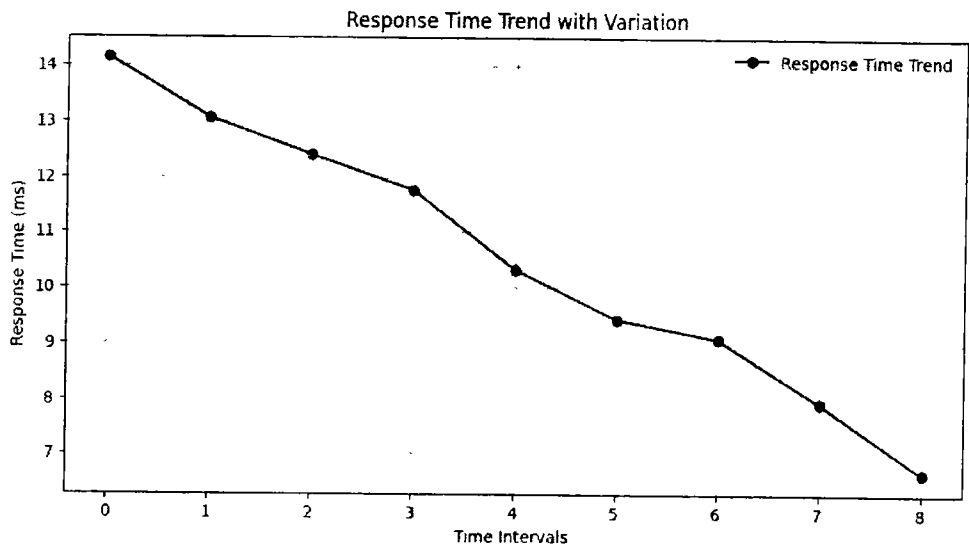


Figure 6.9: Latency Trends

Figure 6.9 present the latency trends over time. The energy efficiency of a system, especially in UWSNs, is of paramount importance, given the challenges associated with recharging or replacing underwater nodes.

The energy consumption distribution is the energy consumed by sensing, processing, communication, and idle. Scalability ensures that as the network grows, the mechanism can handle the increased load without compromising performance. In summation, the proposed mechanism's network performance metrics underscore its robustness and

adaptability. When benchmarked against contemporary research, it emerges as a front-runner, promising enhanced network performance and reliability in UWSNs.

6.5 Chapter Summary

In the chapter, we addressed node mobility issues of UWSNs, by presenting the trust evaluation framework and comparing the proposed with Jang, Goyal, and Zhang's approaches. The experimental results show that the proposed approach based on a modified decision tree is reliable, capable, and secure. Also surpasses existing models in accuracy, energy conservation, and adaptability. Additionally, the proposed system's dynamic update capability allows for real-time responsiveness to changing network conditions, further solidifying its practicality.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

This thesis explores the multifaceted aspects of key management with generalized signcryption and trust evaluation in Underwater Wireless Sensor Networks (UWSNs), a critical area given the unique operational challenges of UWSNs such as limited bandwidth, high latency, and node mobility. The research commenced by investigating the computational efficiency of the key management framework, recognizing the need for lightweight frameworks that can dynamically manage cryptographic keys like key generation, key distribution, and key revocation with minimal computational overhead. The computational burdens associated with adaptive key management and proposed an integrated framework for efficient key generation, distribution, and revocation. The study focused on enhancing scalability and reducing the computational load, thereby improving efficiency for cloud storage applications. In terms of secure communication among sensor nodes cluster heads and sink nodes the traditional "sign-then-encrypt" methodology for UWSNs, discusses its unsuitability for resource-constrained underwater environments due to its high computational and communication costs. The lack of literature on heterogeneous network models and the need for a generalized signcryption approach for secure communication that accounts for the diverse roles and capacities of underwater sensor nodes. Node mobility issue solved by using trust management model. Sensor nodes move from one network to another network creating trust issues. The real-time parameters are collected and calculate trusted values. The sink nodes share trusted values among sink nodes. The moved sensors are easy to become trusted nodes in the networks. So the trust-based management framework for UWSNs, aims to establish node trustworthiness amidst challenges like node mobility and the hostile underwater environment. It highlighted the inadequacies of current trust evaluation mechanisms and presented a forward-secure and publicly verifiable trust management scheme.

7.2 Future Direction

An optimized key management approach with additional compression mechanism and continuous efforts can be made to refine the integrated key management framework, focusing on real-world deployment challenges, adaptive algorithms for key distribution in response to node mobility, and energy-efficient key revocation methods. Future work should also delve into the development of key management and secure communication protocols that are tailored to the heterogeneous nature of UWSNs. This includes exploring algorithms that can adapt to the varying computational and communication capacities of different nodes. There is a substantial opportunity for developing comprehensive trust models that incorporate machine learning to predict node behaviors and adapt to changing conditions. Such models can further be validated through extensive simulations and real-world pilot tests. Investigating the potential integration of emerging technologies such as blockchain and quantum key distribution within UWSNs can also be a promising direction. This includes assessing the viability of these technologies in underwater conditions and their impact on the overall network performance.

References

- [1] H. Luo, X. Wang, Z. Xu, C. Liu, and J.-S. Pan, "A software-defined multi-modal wireless sensor network for ocean monitoring," *International Journal of Distributed Sensor Networks*, vol. 18, no. 1, pp. 15-50, 2022.
- [2] A. Al Guqhaiman, O. Akanbi, A. Aljaedi, and C. E. Chow, "A survey on MAC protocol approaches for underwater wireless sensor networks," *IEEE Sensors Journal*, vol. 21, no. 3, pp. 3916-3932, 2020.
- [3] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, "Internet of Underwater Things and Big Marine Data Analytics—A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 904-956, 2021.
- [4] H. Yang, B. Liu, F. Ren, H. Wen, and C. Lin, "Optimization of Energy Efficient Transmission in Underwater Sensor Networks," in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications*, vol. 2, no. 2, pp. 1-6, 2019.
- [5] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 48-60, 2004.
- [6] S. Fattah, A. Gani, I. Ahmedy, M. Y. Idris, and I. A. Targio Hashem, "A Survey on Underwater Wireless Sensor Networks: Requirements, Taxonomy, Recent Advances, and Open Research Challenges," *Sensors*, vol. 20, no. 18,
- [7] A. M. Almuhaideb, "Re-AuTh: Lightweight re-authentication with practical key management for wireless body area networks," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8189-8202, 2021.
- [8] P. Singh and A. K. Pandey, "A Review on Cloud Data Security Challenges and existing Countermeasures in Cloud Computing," *International Journal of Data Informatics and Intelligent Computing*, vol. 1, no. 2, pp. 23-33, 2022.
- [9] M. Masud *et al.*, "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15694-15703, 2020.
- [10] S. S. Chaeikar, M. Alizadeh, M. H. Tadayon, and A. Jolfaei, "An intelligent cryptographic key management model for secure communications in distributed industrial intelligent systems," *International Journal of Intelligent Systems*, vol. 37, no. 12, pp. 10158-10171, 2022.
- [11] A. G. Yisa, T. Dargahi, S. Belguith, and M. Hammoudeh, "Security challenges of internet of underwater things: A systematic literature review," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 3, pp. 42-63, 2021.
- [12] A. Albakri, L. Harn, and S. Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN)," *Security and communication networks*, vol. 2, no. 5, pp. 10-25, 2019.
- [13] S. Sankaran, "Lightweight security framework for IoTs using identity based cryptography," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2016: IEEE, pp. 880-886.
- [14] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 729-752, 2018.
- [15] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE communications magazine*, vol. 53, no. 8, pp. 54-60, 2015.

- [16] G. Tabella, N. Paltrinieri, V. Cozzani, and P. S. Rossi, "Wireless sensor networks for detection and localization of subsea oil leakages," *IEEE Sensors Journal*, vol. 21, no. 9, pp. 10890-10904, 2021.
- [17] H. Xiong, Y. Hou, X. Huang, Y. Zhao, and C.-M. Chen, "Heterogeneous Signcryption Scheme From IBC to PKI With Equality Test for WBANs," *IEEE Systems Journal*, 2021.
- [18] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," in *Annual international cryptology conference*, 1997: Springer, pp. 165-179.
- [19] P. N. Kasyoka, M. Kimwele, and S. A. Mbandu, "Efficient certificateless signcryption scheme for wireless sensor networks in ubiquitous healthcare systems," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3349-3366, 2021.
- [20] D. Huang, D. Zhao, L. Wei, Z. Wang, and Y. Du, "Modeling and analysis in marine big data: Advances and challenges," *Mathematical Problems in Engineering*, vol. 2015, 2015.
- [21] K. Saeed *et al.*, "A comprehensive analysis of security-based schemes in underwater wireless sensor networks," *Sustainability*, vol. 15, no. 9, p. 7198, 2023.
- [22] A. Doosti-Aref and H. Arslan, "Resource Allocation Optimization in Multiuser OFDM Relay-Assisted Underwater Acoustic Sensor Networks," *Vehicular Communications*, p. 100625, 2023.
- [23] J. Du, G. Han, C. Lin, and M. Martinez-Garcia, "ITrust: An anomaly-resilient trust model based on isolation forest for underwater acoustic sensor networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 5, pp. 1684-1696, 2020.
- [24] S. Lee, H. J. Jo, A. Cho, D. H. Lee, and W. Choi, "TTIDS: Transmission-Resuming Time-Based Intrusion Detection System for Controller Area Network (CAN)," *IEEE Access*, vol. 10, pp. 52139-52153, 2022.
- [25] B. Zhou, S. Li, Q. Li, X. Sun, and X. Wang, "An efficient and scalable pairwise key pre-distribution scheme for sensor networks using deployment knowledge," *computer communications*, vol. 32, no. 1, pp. 124-133, 2009.
- [26] V. Kumar and N. Malik, "Enhancing the connectivity and resiliency of random key pre-distribution schemes for wireless sensor network," *International Journal of System Assurance Engineering and Management*, vol. 13, no. Suppl 1, pp. 92-99, 2022.
- [27] S. Sun and A. Huang, "A review of security evaluation of practical quantum key distribution system," *Entropy*, vol. 24, no. 2, p. 260, 2022.
- [28] S. Sharma and V. K. Verma, "An integrated exploration on internet of things and wireless sensor networks," *Wireless Personal Communications*, vol. 124, no. 3, pp. 2735-2770, 2022.
- [29] N. Goyal, M. Dave, and A. K. Verma, "SAPDA: secure authentication with protected data aggregation scheme for improving QoS in scalable and survivable UWSNs," *Wireless Personal Communications*, vol. 113, pp. 1-15, 2020.
- [30] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," in *Wireless Sensor Networks: 5th European Conference, EWSN 2008, Bologna, Italy, January 30-February 1, 2008. Proceedings*, 2008: Springer, pp. 305-320.

- [31] L. Batina, N. Mentens, K. Sakiyama, B. Preneel, and I. Verbauwhede, "Low-cost elliptic curve cryptography for wireless sensor networks," in *European Workshop on Security in Ad-hoc and Sensor Networks*, 2006: Springer, pp. 6-17.
- [32] G. Han, Y. He, J. Jiang, N. Wang, M. Guizani, and J. A. Ansere, "A synergetic trust model based on SVM in underwater acoustic sensor networks," *IEEE transactions on vehicular technology*, vol. 68, no. 11, pp. 11239-11247, 2019.
- [33] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *2015 International conference on pervasive computing (ICPC)*, 2015: IEEE, pp. 1-6.
- [34] D. T. Hlavacek, "Synoptic analysis techniques for intrusion detection in wireless networks," Iowa State University, 2015.
- [35] F. Mezrag, S. Bitam, and A. Mellouk, "An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks," *Journal of Network and Computer Applications*, vol. 200, p. 103282, 2022.
- [36] A. Feroz Khan and G. Anandharaj, "A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment: CKMT," *SN Applied Sciences*, vol. 1, no. 12, p. 1575, 2019.
- [37] R. A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, "A perfect security key management method for hierarchical wireless sensor networks in medical environments," *Electronics*, vol. 12, no. 4, p. 1011, 2023.
- [38] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, 2018.
- [39] I. Gholizadeh, E. Amiri, and R. Javidan, "An efficient key distribution mechanism for large scale hierarchical wireless sensor networks," in *2019 27th Iranian Conference on Electrical Engineering (ICEE)*, 2019: IEEE, pp. 1553-1559.
- [40] S. Pamarthi and R. Narmadha, "Adaptive key management-based cryptographic algorithm for privacy preservation in wireless mobile adhoc networks for IoT applications," *Wireless Personal Communications*, vol. 124, no. 1, pp. 349-376, 2022.
- [41] P. Bondada, D. Samanta, M. Kaur, and H.-N. Lee, "Data security-based routing in MANETs using key management mechanism," *Applied Sciences*, vol. 12, no. 3, p. 1041, 2022.
- [42] H. Zhou, K. Lv, L. Huang, and X. Ma, "Quantum network: security assessment and key management," *IEEE/ACM Transactions on Networking*, vol. 30, no. 3, pp. 1328-1339, 2022.
- [43] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, S. Shetty, and A. Alqahtani, "Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications," *IEEE Access*, 2023.
- [44] N. C. Gowda, S. S. Manvi, B. Malakreddy, and P. Lorenz, "BSKM-FC: Blockchain-based secured key management in a fog computing environment," *Future Generation Computer Systems*, vol. 142, pp. 276-291, 2023.
- [45] U. Chatterjee, S. Ray, M. K. Khan, M. Dasgupta, and C.-M. Chen, "An ECC-based lightweight remote user authentication and key management scheme for IoT communication in context of fog computing," *Computing*, vol. 104, no. 6, pp. 1359-1395, 2022.
- [46] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," in *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17*, 1997: Springer, pp. 165-179.

- [47] G. Enos and Y. Zheng, "An ID-based signcryption scheme with compartmented secret sharing for unsigncryption," *Information Processing Letters*, vol. 115, no. 2, pp. 128-133, 2015.
- [48] Z. Liu, G. Yang, D. S. Wong, K. Nguyen, and H. Wang, "Key-insulated and privacy-preserving signature scheme with publicly derived public key," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019: IEEE, pp. 215-230.
- [49] G. Yang, D. S. Wong, and X. Deng, "Analysis and improvement of a signcryption scheme with key privacy," in *Information Security: 8th International Conference, ISC 2005, Singapore, September 20-23, 2005. Proceedings 8*, 2005: Springer, pp. 218-232.
- [50] K. G. Paterson and J. C. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Australasian conference on information security and privacy*, 2006: Springer, pp. 207-222.
- [51] Y. Zhou, Z. Li, F. Hu, and F. Li, "Identity-based combined public key schemes for signature, encryption, and signcryption," in *Information Technology and Applied Mathematics: ICITAM 2017*, 2019: Springer, pp. 3-22.
- [52] M. Stojanovic and J. Preisig, "Underwater acoustic communication channels: Propagation models and statistical characterization," *IEEE communications magazine*, vol. 47, no. 1, pp. 84-89, 2009.
- [53] N. Goyal, M. Dave, and A. K. Verma, "Protocol stack of underwater wireless sensor network: classical approaches and new trends," *Wireless Personal Communications*, vol. 104, pp. 995-1022, 2019.
- [54] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Ad hoc networks*, vol. 3, no. 3, pp. 257-279, 2005.
- [55] S. Kumari, K. K. Singh, P. Nand, G. S. Mishra, and R. Astya, "A Comparative Study of Security Issues and Attacks on Underwater Sensor Network," in *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021*, 2022: Springer, pp. 59-74.
- [56] Y. He, G. Han, J. Jiang, H. Wang, and M. Martinez-Garcia, "A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 3, pp. 811-821, 2020.
- [57] S. A. Ch, N. Uddin, M. Sher, A. Ghani, H. Naqvi, and A. Irshad, "An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography," *Multimedia Tools and Applications*, vol. 74, pp. 1711-1723, 2015.
- [58] X. Yu, F. Li, T. Li, N. Wu, H. Wang, and H. Zhou, "Trust-based secure directed diffusion routing protocol in WSN," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-13, 2022.
- [59] S. Alagarsamy and S. Rajagopalan, "Exponentiated Multiple Message Communication using Certificateless Signcryption for Mobile Network Security," *International Journal of Computer Applications*, vol. 975, p. 8887.
- [60] C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, p. 1550147718824465, 2019.
- [61] J. Qiu, K. Fan, K. Zhang, Q. Pan, H. Li, and Y. Yang, "An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT," *IEEE Access*, vol. 7, pp. 180205-180217, 2019.

- [62] X. Yu, W. Zhao, and D. Tang, "Efficient and provably secure multi-receiver signcryption scheme using implicit certificate in edge computing," *Journal of Systems Architecture*, vol. 126, p. 102457, 2022.
- [63] G. Manikandan and U. Sakthi, "OPTIMAL CLUSTER BASED KEY MANAGEMENT SYSTEM USING SIGNCRYPTION ALGORITHM FOR WIRELESS SENSOR NETWORKS," *Neural Network World*, no. 5, 2018.
- [64] C. Yuan, W. Chen, and D. Li, "A hierarchical identity-based signcryption scheme in underwater wireless sensor network," in *China Conference on Wireless Sensor Networks*, 2017: Springer, pp. 44-54.
- [65] Z. Zhou, B. B. Gupta, A. Gaurav, Y. Li, M. D. Lytras, and N. Nedjah, "An efficient and secure identity-based signature system for underwater green transport system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16161-16169, 2022.
- [66] A. Trichili, C. B. Issaid, B. S. Ooi, and M.-S. Alouini, "A CNN-based structured light communication scheme for internet of underwater things applications," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10038-10047, 2020.
- [67] C.-C. Kao, Y.-S. Lin, G.-D. Wu, and C.-J. Huang, "A study of applications, challenges, and channel models on the Internet of Underwater Things," in *2017 International conference on applied system innovation (ICASI)*, 2017: IEEE, pp. 1375-1378.
- [68] S. Goyal, R. V. Ravi, C. Verma, M. S. Raboaca, and F. M. Enescu, "A Lightweight Cryptographic Algorithm for Underwater Acoustic Networks," *Procedia Computer Science*, vol. 215, pp. 266-273, 2022.
- [69] D. Incebacak, K. Bicakci, and B. Tavli, "Evaluating energy cost of route diversity for security in wireless sensor networks," *Computer Standards & Interfaces*, vol. 39, pp. 44-57, 2015.
- [70] J. Cao, J. Dou, Z. Guo, S. Dong, and H. Xu, "ELT: Energy-level-based hybrid transmission in underwater sensor acoustic networks," in *2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks*, 2013: IEEE, pp. 133-139.
- [71] W. C. Xinbin, "Energy efficient and secure transmission scheme based on chaotic compressive sensing in underwater wireless sensor networks," *Digital Signal Processing*, vol. 81, p. 129, 2018.
- [72] M. N. Patwary, S. J. Nawaz, M. A. Rahman, S. K. Sharma, M. M. Rashid, and S. J. Barnes, "The potential short-and long-term disruptions and transformative impacts of 5G and beyond wireless networks: Lessons learnt from the development of a 5G testbed environment," *IEEE Access*, vol. 8, pp. 11352-11379, 2020.
- [73] X. Pan, Y. Jin, Z. Wang, and F. Li, "A pairing-free heterogeneous signcryption scheme for unmanned aerial vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 19426-19437, 2022.
- [74] S. Hussain, I. Ullah, H. Khattak, M. A. Khan, C.-M. Chen, and S. Kumari, "A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for Industrial Internet of Things (IIoT)," *Journal of Information Security and Applications*, vol. 58, p. 102625, 2021.
- [75] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 39-50, 2019.
- [76] M. Elhoseny and K. Shankar, "Reliable data transmission model for mobile ad hoc network using signcryption technique," *IEEE transactions on reliability*, vol. 69, no. 3, pp. 1077-1086, 2019.

- [77] P. Bhattacharya, P. Mehta, S. Tanwar, M. S. Obaidat, and K.-F. Hsiao, "HeaL: A blockchain-envisioned signcryption scheme for healthcare IoT ecosystems," in *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, 2020: IEEE, pp. 1-6.
- [78] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345-1360, 2011.
- [79] R. W. Anwar, A. Zainal, F. Outay, A. Yasar, and S. Iqbal, "BTEM: Belief based trust evaluation mechanism for wireless sensor networks," *Future generation computer systems*, vol. 96, pp. 605-616, 2019.
- [80] D. Wang, Y. Yi, S. Yan, N. Wan, and J. Zhao, "A node trust evaluation method of vehicle-road-cloud collaborative system based on federated learning," *Ad Hoc Networks*, vol. 138, p. 103013, 2023.
- [81] S. Kaur and V. K. Joshi, "Hybrid Soft Computing Technique Based Trust Evaluation Protocol for Wireless Sensor Networks," *Intelligent Automation & Soft Computing*, vol. 26, no. 2, 2020.
- [82] G. Han, Y. He, J. Jiang, H. Wang, Y. Peng, and K. Fan, "Fault-tolerant trust model for hybrid attack mode in underwater acoustic sensor networks," *IEEE Network*, vol. 34, no. 5, pp. 330-336, 2020.
- [83] G. Han, J. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Transactions on Mobile Computing*, vol. 14, no. 12, pp. 2447-2459, 2015.
- [84] D. Velusamy, G. Pugalendhi, and K. Ramasamy, "A cross-layer trust evaluation protocol for secured routing in communication network of smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 1, pp. 193-204, 2019.
- [85] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based trust model for vehicle-to-everything (V2X)," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 440-450, 2019.
- [86] H. Yang, J. Yuan, H. Yao, Q. Yao, A. Yu, and J. Zhang, "Blockchain-based hierarchical trust networking for JointCloud," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1667-1677, 2019.
- [87] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor-cloud system," *Future Generation Computer Systems*, vol. 109, pp. 573-582, 2020.
- [88] N. Goyal, M. Dave, and A. K. Verma, "Trust model for cluster head validation in underwater wireless sensor networks," *Underwater Technology*, vol. 34, no. 3, 2017.
- [89] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996-2018, 2014.
- [90] S. Xie, G. Hu, X. Wang, C. Xing, and Y. Liu, "A Decision Tree-Based Online Traffic Classification Method for QoS Routing in Data Center Networks," *Security and Communication Networks*, vol. 2022, 2022.
- [91] U. Saeed, S. U. Jan, Y.-D. Lee, and I. Koo, "Fault diagnosis based on extremely randomized trees in wireless sensor networks," *Reliability engineering & system safety*, vol. 205, p. 107284, 2021.
- [92] A. Mazidi, M. Mahdavi, and F. Roshanfar, "An autonomic decision tree-based and deadline-constraint resource provisioning in cloud applications," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 10, p. e6196, 2021.

- [93] S. Mejjaoui and R. F. Babiceanu, "RFID-wireless sensor networks integration: Decision models and optimization of logistics systems operations," *Journal of Manufacturing Systems*, vol. 35, pp. 234-245, 2015.
- [94] N. Li, J.-F. Martínez, J. M. Meneses Chaus, and M. Eckert, "A survey on underwater acoustic sensor network routing protocols," *Sensors*, vol. 16, no. 3, p. 414, 2016.
- [95] L. Vihman, M. Kruusmaa, and J. Raik, "Systematic Review of Fault Tolerant Techniques in Underwater Sensor Networks," *Sensors*, vol. 21, no. 9, p. 3264, 2021.
- [96] S. A. Alhandi, H. Kamaludin, and N. A. M. Alduais, "Trust Evaluation Model in IoT Environment: A Comprehensive Survey," *IEEE Access*, 2023.
- [97] S. Fattah, A. Gani, I. Ahmedy, M. Y. I. Idris, and I. A. Targio Hashem, "A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges," *Sensors*, vol. 20, no. 18, p. 5393, 2020.
- [98] L. F. K. Tani and B. Kadri, "A Last Line Naval Defense System Based on Underwater Wireless Sensor Network," in *2022 6th International Conference on Green Energy and Applications (ICGEA)*, 2022: IEEE, pp. 259-264.
- [99] J. ALSHEHRI, A. ALHAMED, and M. FRIKHA, "THE COUNTERMEASURES OF WIRELESS SENSOR NETWORK THREATS IN IOT SYSTEM," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 19, 2023.
- [100] Z. A. Zukarnain, O. A. Amodu, C. Wenting, and U. A. Bukar, "A survey of Sybil attack countermeasures in underwater sensor and acoustic networks," *IEEE Access*, 2023.
- [101] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Science China Information Sciences*, vol. 65, no. 1, p. 112301, 2022.
- [102] J. Iqbal *et al.*, "A Lightweight and Secure Attribute-Based Multi Receiver Generalized Signcryption Scheme for Body Sensor Networks," *IEEE Access*, vol. 8, pp. 200283-200304, 2020, doi: 10.1109/ACCESS.2020.3035324.
- [103] S. S. Ullah *et al.*, "A Computationally Efficient Online/Offline Signature Scheme for Underwater Wireless Sensor Networks," *Sensors*, vol. 22, no. 14, p. 5150, 2022.
- [104] G. N. Nguyen, N. H. Le Viet, A. F. S. Devaraj, R. Gobi, and K. Shankar, "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 28, p. 100464, 2020.
- [105] A. Paul and S. E. Roslin, "A Brief Study on Security Preserved Data Aggregation Approaches in WSN s," in *2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)*, 2023: IEEE, pp. 1-6.
- [106] S. Park, J. Byun, K.-S. Shin, and O. Jo, "Ocean current prediction based on machine learning for deciding handover priority in underwater wireless sensor networks," in *2020 international conference on artificial intelligence in information and communication (ICAIIIC)*, 2020: IEEE, pp. 505-509.
- [107] J. Wang, W. Yi, M. Yang, J. Ma, S. Zhang, and S. Hao, "Enhance the trust between IoT devices, mobile apps, and the cloud based on blockchain," *Journal of Network and Computer Applications*, vol. 218, p. 103718, 2023.