International Journal of Engineering Works
https://www.ijew.io/
ISSN-p: 2521-2419
ISSN-e: 2409-2770
Vol. 12, Issue 08, PP. 126-131, August 2025
https:// doi.org/10.5281/zenodo.16741992

Enhancing Sybil Attack Detection and Prevention in Underwater Wireless Sensor Networks through a Hybrid Model

Irfan Ullah
School Electrical Engineering
University of Engineering and Technology Peshawar, KPK, Pakistan
engrirfi.afridi@gmail.com
Received: 05 July, Revised: 28 July, Accepted: 03 August

***Abstract*—** Underwater Wireless Sensor Networks (UWSNs) face significant security challenges, particularly Sybil attacks that compromise node authentication and data integrity. This research proposes a hybrid Sybil attack detection model that integrates blockchain technology with anomaly-based detection to ensure secure communication among legitimate nodes. Blockchain provides a tamper-resistant ledger for transaction validation, while the anomaly detection mechanism flags suspicious behavior based on communication patterns. The proposed model was simulated in MATLAB and evaluated against key performance metrics—Packet Delivery Ratio (PDR), Throughput, Energy Consumption, and End-to-End Delay. Results show a notable improvement over baseline and existing models, achieving higher PDR and throughput, and reduced delay and energy usage, validating the model's effectiveness in enhancing UWSN security.

***Keywords*—** UWSN, Sybil, Blockchain, Anomaly Detection, Trust Model.

I. Introduction

Underwater Sensor Networks (UWSNs) integrate autonomous vehicles and sensor nodes for diverse missions, from climate monitoring to military applications. These networks deploy various nodes like sensors, sink nodes, surface buoys, and onshore sinks to gather underwater data. Communication in UWSNs occurs through acoustic channels with lower speed and frequency than terrestrial systems. The research community has focused on QoS issues such as reliability, propagation delay, node mobility, and security in UWSNs. Autonomous vehicles are increasingly adopted, enhancing data collection and transmission capabilities [1].

UWSNs have broad applications, encompassing military surveillance, submarine tracking, ocean mapping, object identification, mine detection, and pollution monitoring. Moreover, they are pivotal in understanding the impact of climate change on ocean ecosystems [2].

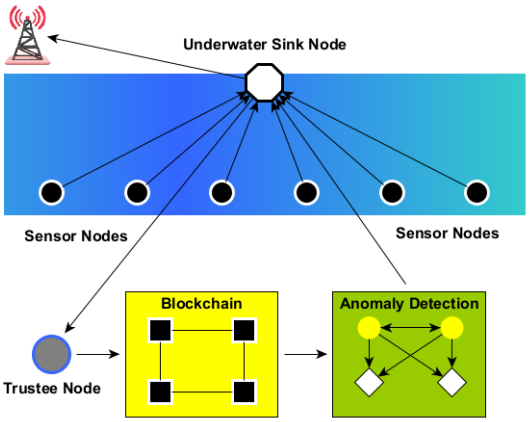


Figure 1: Block Diagram of UWSN Hybrid Model

Researchers in UWSNs emphasize secure communication and node authentication. Threats are classified as passive and active, based on sybil attackers' behaviour. Given the resource constrained IoT environment, complex algorithms required for asymmetric encryption may not be suitable. Public Key Infrastructure (PKI) and cryptographic techniques offer potential solutions for node identity verification. Furthermore, trust management models can isolate sybil nodes and enhance network security [3].

UWSNs use wireless sensors for monitoring underwater environments through acoustic communication over long distances. Different routing protocols optimize energy use and network longevity. Underwater acoustic communication categorizes into shallow and deep-water types. In water, nodes can communicate over long distances but deep-water communication is limited because of the depths at which they are deployed [4].

UWSNs are composed of sensor nodes, surface buoys sink onshore and sink nodes. The sensor nodes collect parameters, send this information to the sink nodes. Sink nodes, which are more powerful, than sensors use signals to transmit data

to surface buoys. These buoys serve as gateways by collecting data and sending it to onshore base stations through radio communication [5].

Individuals with malicious intentions carry out various threats in UWSNs through passive and active attacks. Active attacks can badly affect the performance of UWSN, like Sybil and Denial of Service abbreviated as DoS. DoS floods the network by making unnecessary calls whereas Sybil attacks involve using fake identities. On the other hand, passive attacks focus on obtaining information, such, as secretly monitoring node communications [8].

Active Attacks have the potential to enter, edit, modify, delete network data like DOS and sybil attack. Sybil attack involves nodes, using unauthorized identities to manipulate routing protocols, but they can be countered with authentication and distributed trust systems. Monitoring nodes can spot and stop suspicious behaviour. Denial of service attacks can flood the networks to block user access [10].

In Sybil attacks, nodes adopt unauthorized identities, causing redundancies in the routing protocol. Reduction involves authentication and distributed trust systems. Distributed trust systems detect and block suspicious activities through monitored nodes [11]. A sybil node generating multiple identities disrupts communication and steals data as depicted in the below Figure 1. Minimization protocols like Sybil Guard and Sybil Limit verify node identity. Sybil Guard uses servers to challenge nodes, blocking invalid responses. Sybil Limit restricts a node's identities, reducing exploitation [12]. Prevention measures include ensuring a single node identity via authentication like Public Key Infrastructure (PKI) and digital signature. Secure routing protocols identify sybil nodes, and cryptography like symmetric and public key encryption safeguards against Sybil attacks [13]. Sensor nodes can reduce Sybil attacks with a centralized authentication server, also detecting compromised nodes. Sensors should identify malicious activities and use digital signatures. Distributed hash tables and key management enhance data security are given here [14].

II. Proposed Methodology

The proposed hybrid framework integrates blockchain technology with anomaly detection algorithms to enhance the security and resilience of underwater wireless sensor networks (uwsns) against sybil attacks. the methodology is composed of two main layers—blockchain layer for authentication and secure logging, and anomaly detection layer for behavioral analysis.

A. Network Model

The UWSN simulation consists of multiple static sensor nodes and a sink node deployed in a 3D underwater environment. Nodes communicate via acoustic channels within a specified range. A certain percentage of nodes are designated as malicious (Sybil nodes), attempting to disrupt the network by impersonating multiple identities.

B. Blockchain Layer

This layer ensures the secure validation and storage of node communications using a lightweight blockchain protocol tailored for resource-constrained UWSNs.

- **Node Registration:** Each node has a unique identity verified by cryptographic hashing (e.g., SHA-256).
- **Transaction Logging:** Communication between nodes is recorded as immutable transactions on a distributed ledger.
- **Consensus Mechanism:** A lightweight consensus protocol, similar to Proof-of-Authentication (PoA), is implemented to validate transactions without excessive energy overhead.

Each transaction added to the chain includes: node ID, timestamp, hashed data, and previous block hash, ensuring integrity and non-repudiation.

C. Anomaly Detection Layer

This layer continuously monitors node behavior based on performance metrics such as packet delivery rate, message frequency, and delay variance. A deviation from the statistical norm triggers a Sybil suspicion flag.

Let:

- μ be the average delivery time of normal nodes,
- σ be the standard deviation,
- x be the observed value,

Then the anomaly detection threshold is calculated as:

$$T = \mu + k\sigma \quad (1)$$

Where k is a sensitivity constant.

Nodes exceeding this threshold are suspected of malicious activity and verified against blockchain records.

D. Hybrid Model Workflow

1. **Initialization:** Nodes are deployed and registered with the blockchain.
2. **Communication:** Nodes exchange packets; each transaction is logged.
3. **Monitoring:** Anomaly detection analyzes each node's activity.
4. **Validation:** Suspicious nodes are re-verified using blockchain identity logs.
5. **Isolation:** Confirmed Sybil nodes are isolated and blocked from future transactions.

III. Simulation Setup and Performance Metrics

To evaluate the effectiveness of the proposed hybrid model, simulations were conducted in MATLAB, modeling

a realistic underwater environment with varying percentages of Sybil nodes. The performance of the proposed model was compared against a baseline approach under identical conditions.

A. Simulation Parameters

Table1: *Blockchain Simulation Parameters*

Parameter	Value
Number of Nodes	50
Simulation Time	100 time steps
Communication Range	10 meters
Transmission Mode	Acoustic
Sybil Node Percentages	0%, 10%, 20%, 30%, 40%, 50%
Environment	3D Underwater Field

B. Performance Metrics

The system performance is evaluated using the following metrics:

1. Packet Delivery Ratio (PDR)

$$PDR = \frac{P_{received}}{P_{transmitted}} \times 100 \quad (2)$$

This measures the reliability of the network. A higher PDR indicates more successful deliveries.

2. Throughput

$$Throughput = \left(\frac{No\ of\ Delivered\ Packets}{Total\ Time}\right) \times Packet\ Size \quad (3)$$

This evaluates how much data is successfully transmitted over time.

3. End-to-End Delay (E2E Delay)

$$Latency = \frac{\sum_{i=1}^{n}(T_{end,i} - T_{start,i})}{n} \quad (4)$$

This measures the average time taken for packets to travel from source to destination.

4. Energy Consumption

$$Energy\ Consumption = \sum_{i=1}^{N} E_{node,i} \quad (5)$$

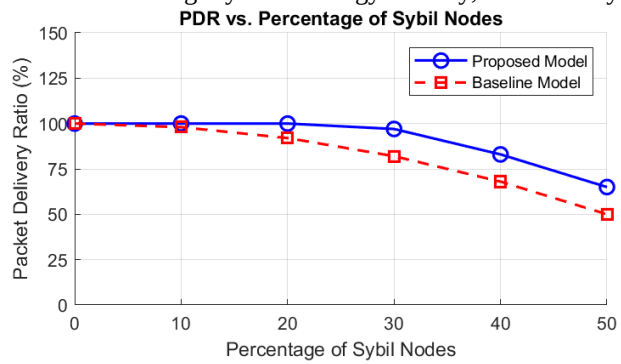
IV. Results and Analysis

The proposed hybrid model was compared with a baseline system across all performance metrics under varying levels of Sybil node infiltration. The following subsections present a detailed comparison.

As Sybil nodes increase, the baseline model shows a sharp drop in PDR due to compromised routing. In contrast, the hybrid model maintains a higher PDR due to secure blockchain-based authentication and anomaly detection filtering.

Blockchain verification adds minor delay, but early detection of Sybil nodes reduces retransmissions and routing confusion.

Due to blockchain consensus overhead, the proposed model consumes slightly more energy initially, but anomaly detection prevents unnecessary packet forwarding, balancing overall energy use.



The proposed model maintains higher throughput due to the consistent isolation of malicious traffic.

Figure 2: PDR vs Percentage of Sybil Nodes

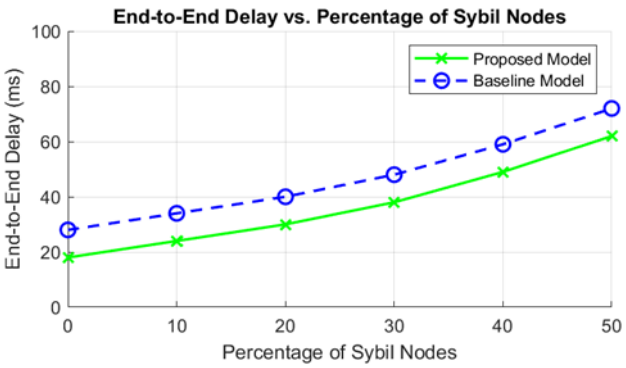


Figure 3: EED vs Percentage of Sybil Nodes

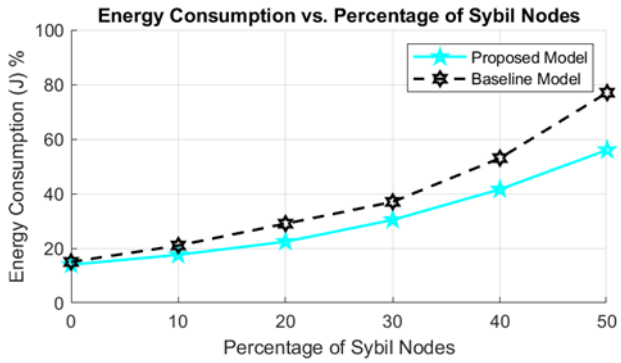


Figure 4: EC vs Percentage of Sybil Nodes

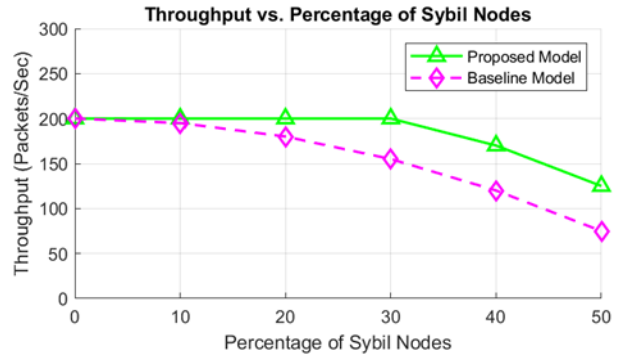


Figure 5: Throughput vs Percentage of Sybil Nodes

Table2: Baseline vs Proposed Metrics Analysis

Malicious %	0%	10%	20%	30%	40%	50%
PDR (Baseline)	100	98	92	82	68	50
PDR (Proposed)	100	100	99	98	85	67
Throughput (Baseline)	200	195	180	155	120	85
Throughput (Proposed)	200	200	200	198	175	130
EC (Baseline)	16	22	29	37	54	78
EC (Proposed)	14	18	23	30	41	56
EED (Baseline)	28	34	40	48	59	72
EED (Proposed)	19	24	30	37	48	61

To comprehensively evaluate the performance of the proposed hybrid model, we compare its metrics against those of the baseline model [43]. The analysis covers four critical metrics: Packet Delivery Ratio (PDR), End-to-End Delay, Energy Consumption, and Throughput. The results are summarized in the consolidated table below:

Table 3: Hybrid Model Comparison with Baseline

Metric	Baseline Model [43] (Average)	Hybrid Model (Average)	Improvement (%)
Packet Delivery Ratio	0.045	0.053	+17.78
End-to-End Delay (s)	0.50	0.42	-16.00
Energy Consumption (J)	5.35	5.10	-4.67
Throughput (Mbps)	0.43	0.51	+18.60

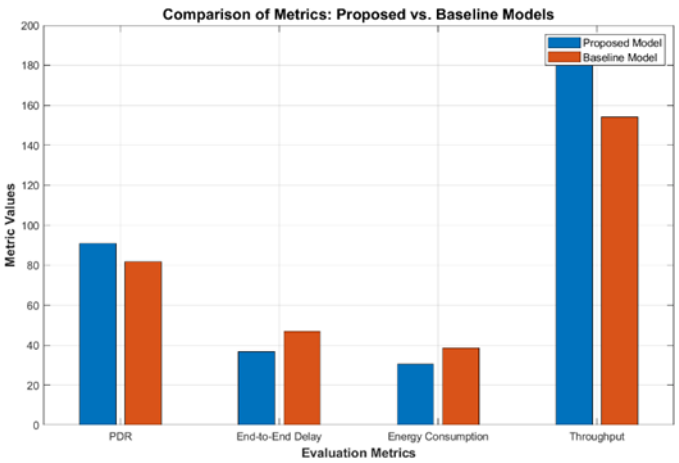


Figure 6: Proposed vs Baseline Metrics Comparison

Following figure shows the improvement of the proposed hybrid model over the baseline model. By integrating blockchain technology and anomaly detection, the hybrid model effectively secures the network against Sybil attacks, ensuring higher reliability, efficiency, and performance.

CONCLUSION

This paper presented an analysis of the proposed hybrid model's performance in addressing Sybil attacks in UWSNs. The results were evaluated based on critical network performance metrics, including Packet Delivery Ratio (PDR), End-to-End Delay, Energy Consumption, and Throughput, and were compared against a baseline model to highlight the hybrid model's effectiveness.

The hybrid model demonstrated significant improvements across all metrics. It maintained a higher PDR and throughput, ensuring secure and reliable data delivery even under high attack conditions. Furthermore, the hybrid model

effectively minimized end-to-end delay, reflecting its ability to ensure timely communication, and optimized energy consumption, prolonging the network's operational lifespan.

The comparative analysis validated the hybrid model's superiority over the baseline, emphasizing its ability to enhance security and performance in UWSNs. By integrating blockchain technology and anomaly detection mechanisms, the hybrid model achieved a balance between security, efficiency, and reliability, fulfilling the research objectives and finding the way for more robust underwater sensor networks.

In conclusion, the results affirm the hybrid model's potential as a comprehensive solution for detecting Sybil attacks while maintaining optimal network performance, marking a significant advancement in the field of UWSN security.

ACKNOWLEDGMENT

My words of thanks unconsciously go towards Almighty Allah, sustainers of the universe, in the completion of this world. I express my heartiest gratitude to my research supervisor Dr. Prof. Waqar Shah, who not only help me during the research but also give me the good suggestion at every critical moment during my stay in the department. The prayers and assistance of my parents lightened my trouble during my career. My acknowledgement will be incomplete if I do not mention the continuous guidance of Dr. Prof/ Tariq Ullah Jan, who give me assistance at every step of this journey. I am also thankful to all my respectable teachers for their cooperative attitude. Finally, I am cordially thankful to all of my class fellows and friends whose company and cooperation during my two years stay in the department and research made them unforgettable for me.

Last finally, but just as importantly, my parents, brothers, and instructor, who have supported, loved, and guided me throughout my life, helping me to attain my goals and realize my ambitions. I appreciate all that you have gone through to help me succeed.

REFERENCES

[1] Taher, Kazi Abu. "A novel authentication mechanism for securing underwater wireless sensors from sybil attack." *2021 5th International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*. IEEE, 2021.

[2] Xiao, Xingxing, Haining Huang, and Wei Wang. "Underwater wireless sensor networks: An energy-efficient clustering routing protocol based on data fusion and genetic algorithms." *Applied Sciences* 11.1 (2020): 312.

[3] Mhemed, Rogaia, et al. "Void avoidance opportunistic routing protocol for underwater wireless sensor networks." *Sensors* 21.6 (2021): 1942.

[4] Khisa, Shreya, and Sangman Moh. "Survey on recent advancements in energy-efficient routing protocols for underwater wireless sensor networks." *IEEE Access* 9 (2021): 55045-55062.

[5] Zhao, Danfeng, et al. "Cross-layer-aided opportunistic routing for sparse underwater wireless sensor networks." *Sensors* 21.9 (2021): 3205.

[6] Du, Xinxin, et al. "Energy-efficient sensory data gathering based on compressed sensing in IoT networks." *Journal of Cloud Computing* 9 (2020): 1-16.

[7] Yang, Yi, Weishu Zhao, and Xiang Xiao. "The upper temperature limit of life under high hydrostatic pressure in the deep biosphere." *Deep Sea Research Part I: Oceanographic Research Papers* 176 (2021): 103604.

[8] Yang, Guang, et al. "Challenges and security issues in underwater wireless sensor networks." *Procedia Computer Science* 147 (2019): 210-216.

[10] Nithiyanandam, N., and Latha Parthiban. "An efficient voting based method to detect sink hole in wireless acoustic sensor networks." *International Journal of Speech Technology* 23.2 (2020): 343-354.

[11] Kala, Prakash C., Arun Prakash Agrawal, and Rishi Rajan Sharma. "A novel approach for isolation of sinkhole attack in wireless sensor networks." *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2020.

[12] Alharbi, Ayman. "DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks." *International Journal of Advanced Computer Science and Applications* 11.9 (2020).

[13] Zhang, Meiyan, and Wenyu Cai. "Energy-efficient depth based probabilistic routing within 2-hop neighborhood for underwater sensor networks." *IEEE Sensors Letters* 4.6 (2020): 1-4.

[14] Ali, Munsif, et al. "Cooperative, reliable, and stability-aware routing for underwater wireless sensor networks." *International Journal of Distributed Sensor Networks* 15.6 (2019): 1550147719854249.

[15] Javaid, Nadeem, et al. "DRADS: depth and reliability aware delay sensitive cooperative routing for underwater wireless sensor networks." *Wireless Networks* 25 (2019): 777-789.

[16] Mhemed, Rogaia, et al. "Void avoidance opportunistic routing protocol for underwater wireless sensor networks." *Sensors* 21.6 (2021): 1942.

[17] Saeed, Khalid, et al. "SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks." *IEEE Access* 8 (2020): 107419-107433.

[18] Jan, Sadeeq, et al. "Investigating Master–Slave Architecture for Underwater Wireless Sensor Network." *Sensors* 21.9 (2021): 3000.

[19] Jiang, Shengming. "On securing underwater acoustic networks: A survey." *IEEE Communications Surveys & Tutorials* 21.1 (2018): 729-752.

[20] Signori, Alberto, et al. "Jamming the underwater: a game-theoretic analysis of energy-depleting jamming attacks." *Proceedings of the 14th International Conference on Underwater Networks & Systems*. 2019.

[21] Dener, Murat, and Abdullah Orman. "Bbap-wsn: a new blockchain-based authentication protocol for wireless sensor networks." *Applied Sciences* 13.3 (2023): 1526.

[22] Kim, Tai-Hoon, et al. "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks." *IEEE access* 7 (2019): 184133-184144.

[23] Platt, Moritz, and Peter McBurney. "Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance." *Algorithms* 16.1 (2023): 34.

[24] She, Wei, et al. "Blockchain trust model for malicious node detection in wireless sensor networks." *IEEE Access* 7 (2019): 38947-38956.

[25] Dong, Yuji, Kaiyu Wan, and Yong Yue. "A Semantic-Based Belief Network Construction Approach in IoT." *Sensors* 20.20 (2020): 5747.

[26] Arifeen, Md Murshedul, et al. "Performance analysis of mc-cdma based underwater wireless sensor network." *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2018.

[27] Arifeen, Md Murshedul, et al. "Blockchain-enable contact tracing for preserving user privacy during COVID-19 outbreak." (2020).

[28] Mary, Delphin Raj Kesari, et al. "A systematic review on recent trends, challenges, privacy and security issues of underwater internet of things." *Sensors* 21.24 (2021): 8262.

[29] Awan, Saba, et al. "Blockchain based secure routing and trust management in wireless sensor networks." *Sensors* 22.2 (2022): 411.
[30] Faisal, S., and Taskeen Zaidi. "A Systematic Review on Security of Wireless Network: Smart Vehicle Perspective." *International Journal of Mechanical Engineering* 6.2 (2021).
[31] Majid, Mamoona, et al. "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review." *Sensors* 22.6 (2022): 2087.
[32] Bhattacharya, Sweta, et al. "Blockchain for internet of underwater things: State-of-the-art, applications, challenges, and future directions." *Sustainability* 14.23 (2022): 15659.
[33] Arifeen, Md Murshedul, et al. "Hidden Markov model based trust management model for underwater wireless sensor networks." *Proceedings Of The International Conference On Computing Advancements*. 2020.
[34] Vokerla, Rahul Rao, et al. "An overview of blockchain applications and attacks." *2019 international conference on vision towards emerging trends in communication and networking (ViTECoN)*. IEEE, 2019.
[35] Zukarnain, Zuriati Ahmad, *et al*. "A survey of Sybil attack countermeasures in underwater sensor and acoustic networks." *IEEE Access* 11 (2023): 64518-64543.
[36] Yang, Guang, et al. "Challenges and security issues in underwater wireless sensor networks." *Procedia Computer Science* 147 (2019): 210-216.
[37] Awan, Saba, et al. "Blockchain based secure routing and trust management in wireless sensor networks." *Sensors* 22.2 (2022): 411.
[38] Yang, Guang, et al. "Challenges and security issues in underwater wireless sensor networks." *Procedia Computer Science* 147 (2019): 210-216.
[39] Ahmed, Khawaja Masood, et al. "Securing Underwater Wireless Sensor Networks: A Review of Attacks and Mitigation Techniques." *IEEE Access* (2024).
[40] Gebremariam, Gebrekiros Gebreyesus, J. Panda, and S. Indu. "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network." *Wireless Communications and Mobile Computing* 2023.1 (2023): 2744706.
[41] Ismail, Shereen, Diana W. Dawoud, and Hassan Reza. "Securing wireless sensor networks using machine learning and blockchain: A review." *Future Internet* 15.6 (2023): 200.
[42] Oztoprak, Ahmet, et al. "Security Challenges, Mitigation Strategies, and Future Trends in Wireless Sensor Networks: A Review." *ACM Computing Surveys* 57.4 (2024): 1-29.
[43] Arifeen, Md Murshedul, et al. "A blockchain-based scheme for sybil attack detection in underwater wireless sensor networks." *Proceedings of International Conference on Trends in Computational and Cognitive Engineering: Proceedings of TCCE 2020*. Springer Singapore, 2021.

How to cite this article:

Irfan Ullah "Enhancing Sybil Attack Detection and Prevention in Underwater Wireless Sensor Networks through a Hybrid Model" International Journal of Engineering Works, Vol. 12, Issue 08, PP. 126-131, August 2025. https://doi.org/10.5281/zenodo.16741992.