International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

Underwater Acoustic Sensor Networks for Secure Communication

Mr. Ravindra P Dhongadi[1], Dr. S.M. Hirikude[2]
[1]Research Scholar, Sanjay Ghodawat University, Atigre, Maharashtra, India.
[2]Head of Electronics & Communication Engineering Department, Sanjay Ghodawat University, Atigre, Maharashtra, India.
Emails: *ravindra.dhongadi@sgipolytechnic.in[1], swapni.hirikude@sanjayghodawatuniversity.ac.in[2]*

Abstract
Underwater Acoustic Sensor Networks (UASNs) are gaining increasing interest from researchers due to their promising applications in areas like oil spill monitoring, maritime surveillance, deep-sea archaeology, and marine environment monitoring. With approximately 70% of the Earth's surface covered by water, accessing valuable data from the seafloor is challenging without the aid of specialized technology. Sensor nodes are used in UWSNs to monitor the underwater environment. Once data is collected, it is sent to a sink node, which forwards it to a base station for additional processing. However, sensor node deployment in UWSNs is challenging due to the harsh underwater circumstances, and issues like high energy consumption and restricted communication range make data routing more complicated. UASNs are vulnerable to attacks from malicious nodes, including wormhole, black hole, and Sybil attacks. Lightweight cryptography, which focuses on algorithms that consume less memory, processing power, and energy, is ideal for resource-constrained devices like smartphones, sensors, and IoT devices. One such method that has been used is the Hénon map, a chaotic system, which is particularly useful for text and image encryption. It offers a balance between security and resource efficiency by generating random sequences that drive encryption techniques on devices with limited processing power.

Keywords: *Underwater Acoustic Sensor Networks (UASNs), underwater vehicle networks (AUVNs), TPR (True Positive Rate), FPR (False Positive Rate).*

1. Introduction
Communication techniques that use acoustic signals to go from one location to another are known as acoustic communications. The only physically practical instrument that functions in an underwater environment is an acoustic signal. Electromagnetic waves can only reach a limited distance under water because of the severe attenuation and absorption impact of the underwater environment [1]. It is discovered that seawater absorbs roughly 45× f dB per kilometer of electromagnetic energy, where f is the frequency in Hertz. However, compared to most frequencies of interest, the absorption of acoustic signals is approximately three orders of magnitude lower. The use of optical signals for underwater applications is being investigated [2]. They discover, however, that in extremely clean water environments (deep water, for instance), optical signals can only go a certain distance. Therefore, it is not a suitable instrument for long-distance transmission in environments with unclean water, such as shallow water, or underwater. UASNs and autonomous underwater vehicle networks (AUVNs) are examples of underwater acoustic networks, which are networks with more than two nodes that use acoustic signals to communicate for underwater applications [3]. Two significant types of UANs are UASNs and AUVNs. The former is mostly used for monitoring and is made up of several sensor nodes. Usually, the nodes have little or no ability to move.

1.1. Underwater Acoustic Sensor Networks (UASN)
Underwater wireless networks are utilized for a variety of military, environmental, and industrial applications, including monitoring beneath the seas and oceans [4]. For instance, an underwater observatory is required to track submarines and locate pollutant sources. Additional uses include underwater monitoring for the discovery of natural

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

resources including minerals, oil, and gas. Sensors in the undersea space are required to keep an eye on these applications (Figure 1).

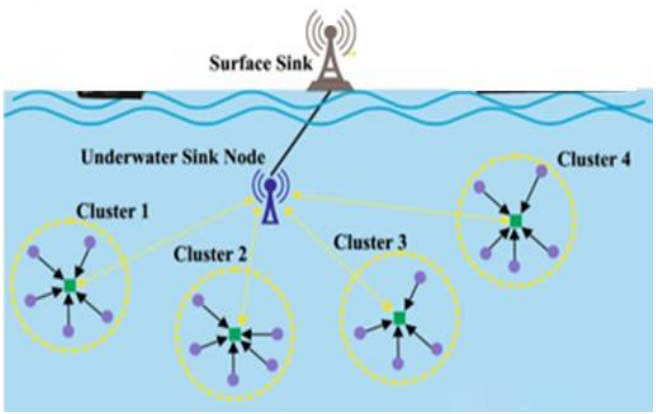

Figure 1 Overview of UASN

1.2.UWSNs Security Threats

Among the risks to underwater Acoustic sensor networks (UASNs) are the following:

- **Denial of Service:** To take up network bandwidth and stop authorized users from using resources, a lot of requests are issued.
- **Wormhole:** The original message is copied and sent again, either in full or in part [5].
- **Sybil:** A malicious node communicates with different nodes by using numerous identities.
- **A black hole:** A rogue node gives fake route information to target nodes so they can gain a replay.
- **Selective Forwarding:** After receiving data, a rogue node drops it by pretending to be a legitimate node.
- **Node Destruction:** A malevolent node renders a node inoperable and assumes its identity [6-8].
- **Sinkhole:** For the network to obtain full data from the base station, a new node is added.
- **Eavesdropping:** Information sent over a network can be overheard by intruders [9].

1.3.Objective

- Offer a dependable routing protocol with node authentication that is appropriate for maritime applications' communication needs [10]. Node authentication will be employed to safeguard the security and privacy of critical data.
- Malicious node attack detection and prevention: By reducing a network's reaction time and throughput, malicious node attacks might impair its functionality. Techniques like "fuzzy logic," which assesses the dependability of nodes based on their interactions, historical behavior, and other criteria, can be used to identify and stop malevolent nodes [11].
- By adding cryptographic algorithms that overcome the lightweight security over communication, you may achieve maximum security and make associated metric performance analysis [12]. To guarantee the confidentiality and integrity of underwater communication, the security framework uses testing and simulations on actual data. It includes several cryptography methods and a secure routing protocol.

1.4.Routing

To carry the simulation experiment 100 nodes deployed in random position sufficient enough to be in communication range of each node (Table 1). Following are the simulation parameters:

Table 1 Experimental Simulation Parameters

Network Dimensions	10 x 10 x 10 (km^3)
Nodes	100
Sink	1
Initial Node Energy	10 (Joule)
Transmission range	1.2 (Km)
Transmission Energy	50 (mJ)
Receiving Energy	30 (mJ)
Data Rate	16 (kbps)
Size of ACK	50 (bits)

Each Node collecting the neighbor information by sending the HELLO message with self-ID, the neighbor nodes send back the self-formation, if the node if authenticated then only it is accepted as neighbor node [13]. By using neighbor information source node sends request to neighbor for shortest path, when it reaches sink, sink send acknowledgement (ACK) back to source. After getting shortest path the data is sent to sink (Table 1).

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

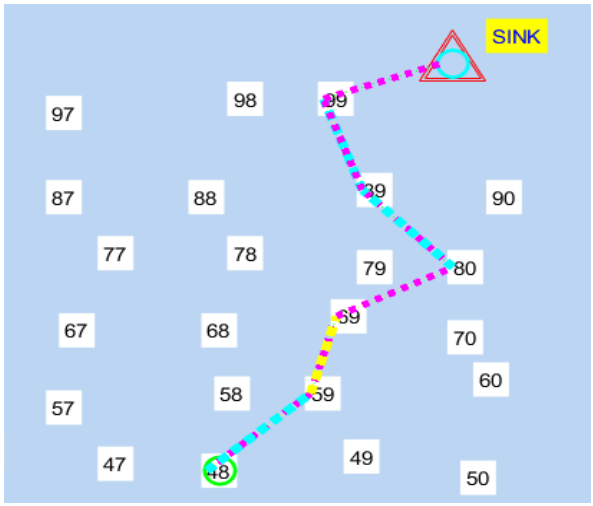

Figure 2 Selecting Routing Path

In Figure 2, node 48 selected as source node, figure shows the routing path selected from source to sink.

2. Malicious Node Detection and Prevention

Fuzzy logic is used in order to identify the rogue node. To identify malicious nodes, we consider the three metrics shown below [14].

- **ETX:** The anticipated quantity of transmissions needed to deliver a packet to its final location. It assesses the transmission's accuracy.
- **Delay:** The typical amount of time it takes for a packet to get to its destination [15].
- **Energy:** The cost of the way's energy as well as the energy of the path node with the lowest remaining battery level.
- **QoS:** Quality of Service of node [16].

Fuzzification process: In order to avoid the challenge of immediately combining the selected three metrics variables into one, we do the fuzzification method in two steps, as shown in figure 3.

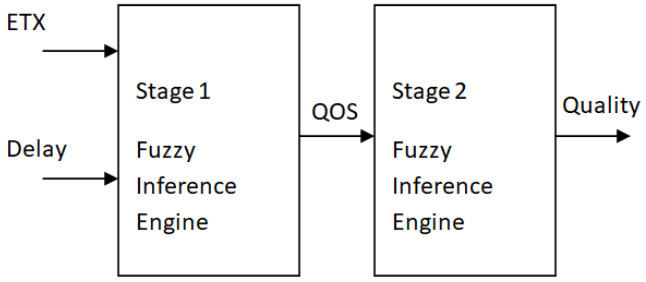

Figure 3 Fuzzy Inference Engine

The first step of fuzzification uses delay and ETX as inputs to compute QoS, which then acts as input for the next level. Table 2 shows the relationship between the ETX and delay variables used in the QoS calculation. This table was created following clear, easy-to-understand guidelines and grounded in specific knowledge.

Table 2. QoS rules

ETX/ Delay	Short	Average	Long
Small	Very Fast	Fast	Moderate
Average	Fast	Moderate	Slow
High	Moderate	Slow	Very Slow

As delay (and ETX) are calculated at the path level, Figure 4 presents their membership functions, normalized based on the number of hops from the sink. Figure 5 Delay Fuzzification Rules with ETX

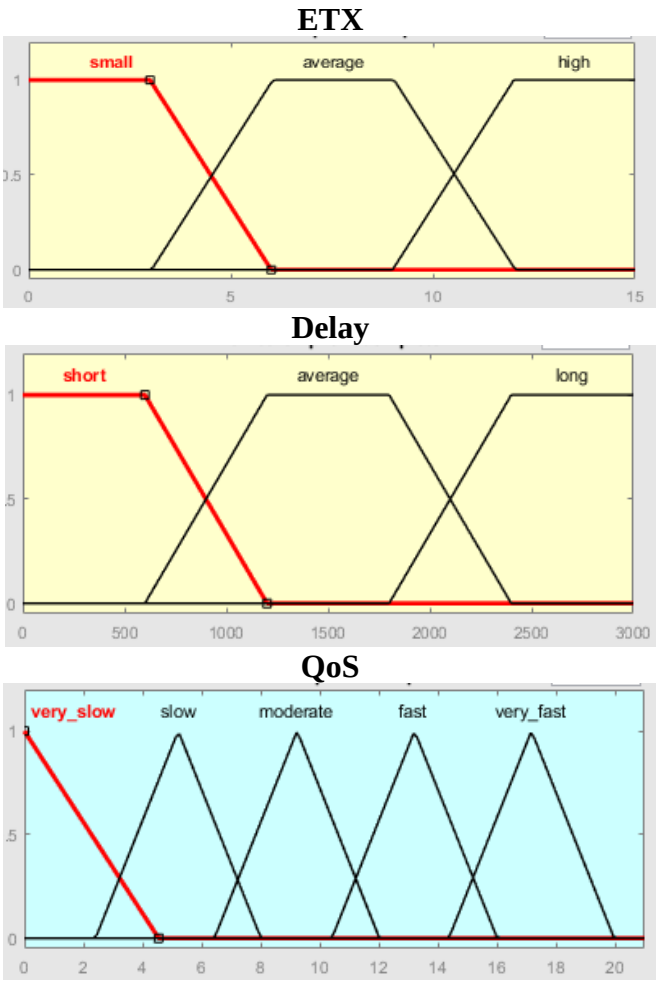

Figure 4 ETX and Delay Membership Functions

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

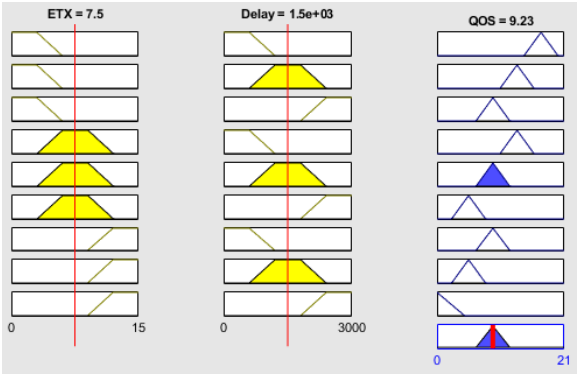

Figure 5 ETX and Delay Fuzzification Rules

Stage 2 Fuzzification: We create QUALITY as the second stage of the fuzzy inference system by integrating the Energy metric variable with the previously determined QoS. Table 3 demonstrates how to calculate Quality using energy and QoS.

Table 3 QUALITY Rules

QoS/ Energy	Low	Medium	Full
Very Slow	Awful	Bad	Average
Slow	Bad	Degraded	Average
Moderate	Degraded	Average	Acceptable
Fast	Average	Acceptabl	Good
Very Fast	Average	Good	Excellent

Figure 6 shows membership function plot for Energy and QUALITY.

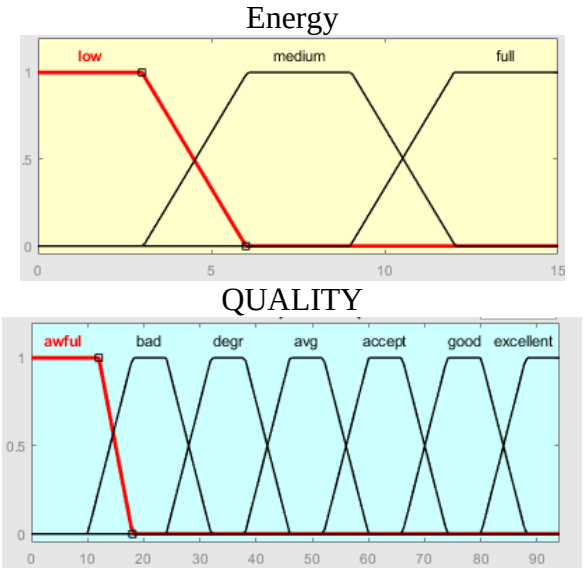

Figure 6 Energy& QUALITY Membership Functions

3. Henon Chaotic Mapping

To make end to end cryptography lightweight Henon Mapping cryptography is used. After sensing the data (Temperature, Light, Image etc) source encrypts the data using preshared key and send to sink. After reaching at sink data is decrypted. Sensed numeric data converted to string. String converted to ASCII codes after applying the henon map the ASCII string encrypted. Again it is converted to Text form and transmitted. Figure 7 shows Henon Encryption Flowchart.

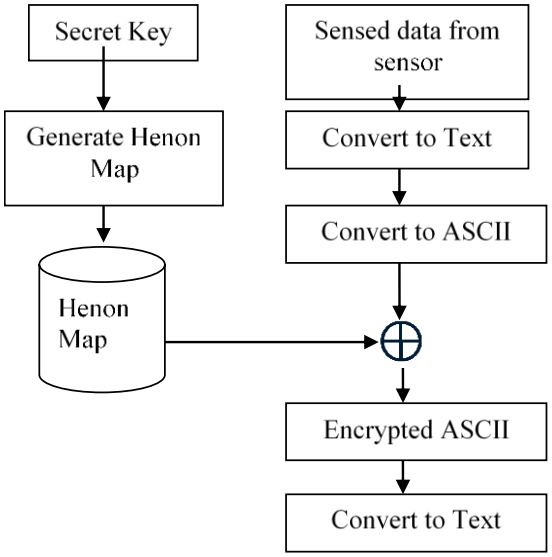

Figure 7 Henon Encryption Flowchart

If sensed data is image it is resized and then directly incremented and transmitted.

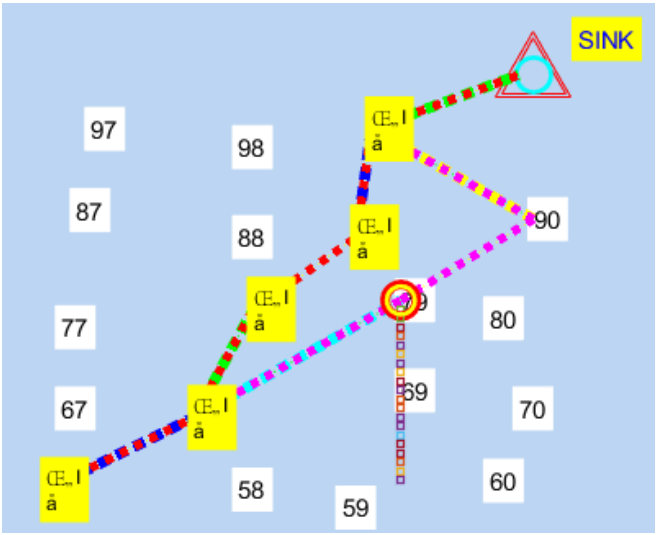

Figure 8 Simulation snapshot

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

In Figure 8, node 57 chosen as source, while finding path node 79 detected as the malicious node. So the route is redirected to a new path discarding the malicious node. The sensed data 4,4.3 (temperature in degree and light in candela) is encrypted and transmitted. On the path yellow patch shows encrypted message at each node on path. Finally, it decrypted at sink.

4. Result and Analysis

We can evaluate the application's dependability in gathering and sending data to the sink, as well as routing stability., and the network's lifespan by monitoring the decline in node energy and tracking the frequency of best parent changes over time (Table 4 & 5). Data security is a key concern, so we are implementing measures to detect and prevent malicious nodes. Additionally, we enhance data security through the use of lightweight cryptography. The performance analysis is divided in three parts:

- Malicious attack detection
- Network Analysis
- Data Security Analysis

To evaluate the malicious detection accuracy. The simulation is run from 50 times and following result found.

Table 4 Malicious Node Detection Analysis

Accuracy of Detection	92.59 %
TPR or Sensitivity	94.23 %
FPR or Specificity	50.00 %

For Network Analysis following metrics are found.

- **Network Life Tim:** This essentially describes how long a network will function before needing to be maintained, repaired, or replaced. Network lifetime is typically measured in time units (e.g., seconds, minutes, hours, and days).
- **Data Transmission Rate:** The data transmission rate refers to the quantity of data or packets transmitted over a specified period of time.
- **Throughput:** The quantity of data that is successfully sent over a network in a specific amount of time is referred to as throughput. It is an important performance indicator that shows how efficiently data packets get transmitted across networks.
- **Energy Consumption:** refers to how much energy computing systems, including data communications infrastructure, power supply, cooling systems, and security technologies, consume.

Table 5 Network Analysis

Network Life Time	32.45 sec
Data Transmission Rate	91.51 Kbps
Throughput	75.48 Kbps
Energy Consumption	1.44 mJ

Data security performance analysis made by using following metrics (Refer Figure 9 to 14 & Table 6).

MSE (Mean Squared Error): By averaging the squared differences of the matching values, the MSE calculates the difference between two data points. It is a widely used statistic to assess encryption and decryption. High MSE is better.

$$MSE = (1 / (m * n)) * \Sigma \Sigma (I(i, j) - K(i, j))^2$$

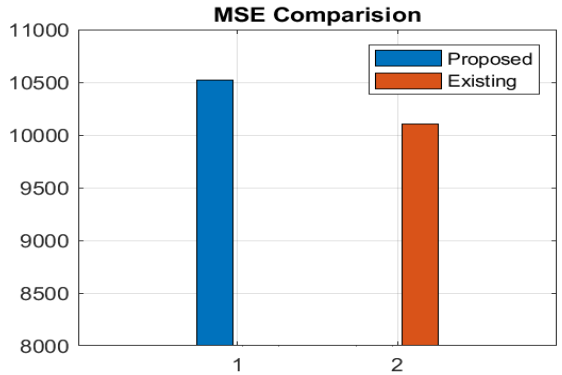

Figure 9 MSE Comparison

Peak Signal-to-Noise Ratio, or PSNR, is a statistic used to assess an encryption's quality. Higher PSNR values often indicate greater image quality and lower noise levels (Figure 10).

$$PSNR = 10 * \log10(R^2 / MSE)$$

where R is the maximum possible pixel value (e.g., 255 for 8-bit grayscale images).

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

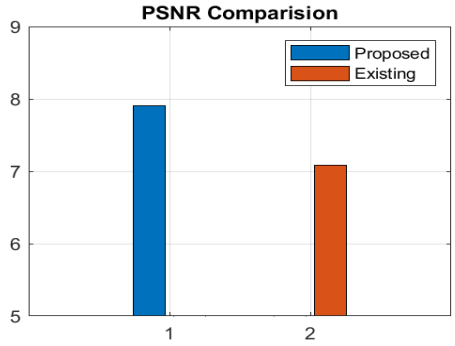

Figure 10 PSNR Comparison

SSIM (Structural Similarity Index): method for determining how similar two images/data are. In image processing, it's frequently used to assess how much an image has been encrypted.

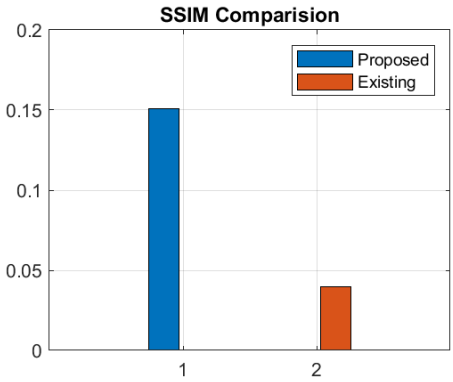

Figure 11 SSIM Comparison

Entropy: In cryptography, the term "entropy" defines the degree of unpredictability or randomness in a system. Whereas low entropy denotes predictability, high entropy suggests that the system is extremely random, making it challenging for attackers to anticipate or forecast values.

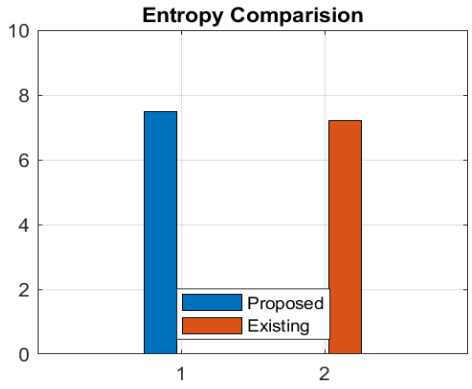

Figure 12 Entropy Comparison

NPCR (Number of Pixels Change Rate): is a measure that assesses how sensitive an encryption technique is to modifications in the input (plaintext). It calculates the proportion of pixel differences between two ciphertexts created from plaintexts that are only one pixel different. Since even minor changes in the input result in notable variations in the output, a high NPCR score denotes a strong resistance to differential attacks.

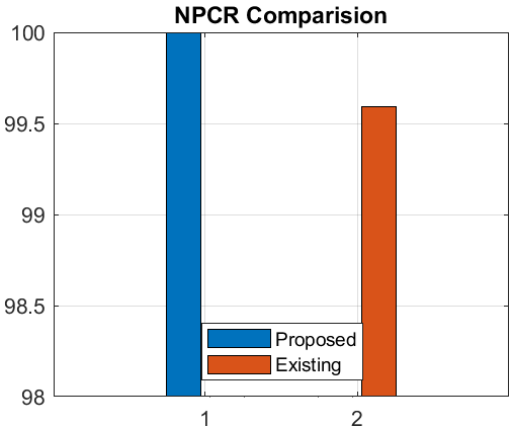

Figure 13 NPCR Comparison

UACI (Unified Average Changing Intensity): is a statistic used to evaluate how sensitive an encryption method is to slight input changes. With the exception of one pixel, it determines the average change in pixel intensity between two encrypted images that are identically the same as the original, unencrypted image. In general, an encryption algorithm with a high UACI value is more resistant to differential assaults.

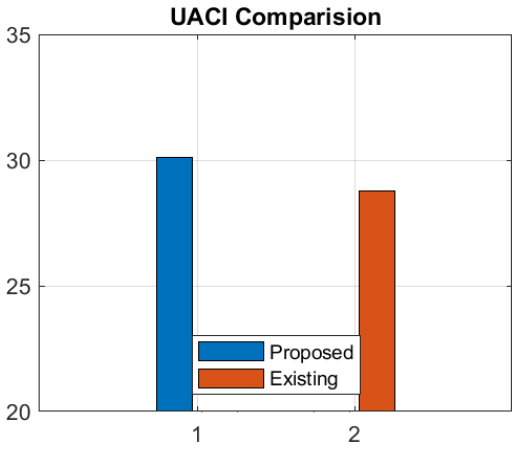

Figure 14 UACI Comparison

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

Table 6 Data Security Analysis

MSE	10521.8
PSNR	7.9099
SSIM	0.15
Entropy	7.50
NPCR	100.00
UACI	30.10

Conclusion

It is more efficient since the routing algorithm selects the path with less hop counts. In order to identify the malicious node, the suggested method employs fuzzy inference methods. It has demonstrated excellent detection and prevention accuracy. Data may be exposed or the system may be attacked by a hostile node if UWSN security rules are not followed. In order to preserve secrecy and integrity while taking into consideration the special features and limitations of the underwater communication network, we have offered a security scenario and an effective encryption technique. The application layer's chaotic Henon Map cryptography technique produces very minimal overhead, which makes it perfect for underwater picture communication, according to simulations and cryptographic testing. The method's ability to meet security requirements was demonstrated through security analysis. We successfully implemented the encryption and decryption methods programmatically, proving that the proposed methodology could achieve private communication. We will look into the possibility of using this technology to encrypt underwater video because of the excellent performance it may offer when encrypting colored imagery.

References

[1]. Taher, R. J., & Mohsen, K. K. (2024). Underwater Wireless Sensor Networks. In BIO Web of Conferences (Vol. 97, p. 00023). EDP Sciences.

[2]. Saeed, K., Khalil, W., Al-Shamayleh, A. S., Ahmed, S., Akhunzada, A., Alharthi, S. Z., & Gani, A. (2023). A comprehensive analysis of security-based schemes in underwater wireless sensor networks. Sustainability, 15(9), 7198.

[3]. Shah, S., Munir, A., Waheed, A., Alabrah, A., Mukred, M., Amin, F., & Salam, A. (2023). Enhancing security and efficiency in underwater wireless sensor networks: a lightweight key management framework. Symmetry, 15(8), 1484.

[4]. Fethi Demim, Rekia Bouguessa, Abdenebi Rouigueb, Abdelkrim Nemra,“ A Systematic Overview of Underwater Wireless Sensor Networks: Applications, Challenge and Research Perspectives” , Journal of Computer Science Research | Volume 05 | Issue 02 | April 2023

[5]. Garg, M., Sharma, S., Balu, V., Sinha, D. K., Bhatt, P., & Bhagat, A. K. (2022). Underwater Acoustic Sensor Network Data Optimization with Enhanced Void Avoidance and Routing Protocol. International Journal of Communication Networks and Information Security, 14(3), 150-162.

[6]. Goyal, S. B., Ravi, R. V., Verma, C., Raboaca, M. S., & Enescu, F. M. (2022). A lightweight cryptographic algorithm for underwater acoustic networks. Procedia Computer Science, 215, 266-273.

[7]. Ateniese, G., Capossele, A., Gjanci, P., Petrioli, C., & Spaccini, D. (2015, May). SecFUN: Security framework for underwater acoustic sensor networks. In OCEANS 2015-Genova (pp. 1-9). IEEE.

[8]. Dini, G., & Lo Duca, A. (2012). A secure communication suite for underwater acoustic sensor networks. Sensors, 12(11), 15133-15158.

[9]. Gussen, C. M., Diniz, P. S., Campos, M. L., Martins, W. A., Costa, F. M., & Gois, J. N. (2016). A survey of underwater wireless communication technologies. J. Commun. Inf. Sys, 31(1), 242-255.

[10]. Ayman Alharbi1 and Muhammad Muzzammil, “A Survey on the Security of Routing Protocols for Underwater Acoustic Sensor Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.22 No.1, January 2022.

[11]. Ayman Alharbi, and Muhammad Muzzammil, “A Survey on the Security of

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 07 July 2025
Page No: 3087 - 3094
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0455

Routing Protocols for Underwater Acoustic Sensor Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.22 No.1, January 2022

[12]. Rehman, Z. U., Altaf, S., & Iqbal, S. (2020). An efficient lightweight key agreement and authentication scheme for WBAN. IEEE Access, 8, 175385-175397.

[13]. Mishachandar, B., & Vairamuthu, S. (2019). A review on underwater acoustic sensor networks: Perspective of internet of things. Int. J. Innovative Technol. Exploring Eng, 8(6), 1603-1615.

[14]. Sweta, S., & Maram, B. (2018). Underwater Wireless Sensor Networks. JOIV: International Journal on Informatics Visualization, 2(1), 10-12.

[15]. SnehalGawde, P., Hajare, V., DhanashreeHirave, P., & Mali, J. Underwater Wireless Communication Using Matlab Simulink.

[16]. Peng, C., Du, X., Li, K., & Li, M. (2016). An Ultra-Lightweight Encryption Scheme in Underwater Acoustic Networks. Journal of Sensors, 2016(1), 8763528.