INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Secure Fuzzy Simple Shortest Path Routing Protocol (SF_SSP) for Underwater Communication

Salma S Shahapur[1]*, **Rajashri Khanai**[2], **D A Torse**[2], **Chinmay Abhay Nerurkar**[3], **H P Rajani**[1]

1 Department of Electronics and Communication Jain College of Engineering, Karnataka,India
2 Department of Electronics and Communication, KLE DR MSSCET college of Engineering and Technology, Karnataka, India
3 Principal Software Engineer, Microsoft, New York, United States

OPEN ACCESS

Received: 08-08-2023

Accepted: 19-10-2023

Published: 21-11-2023

Citation: Shahapur SS, Khanai R, Torse DA, Nerurkar CA, Rajani HP (2023) Secure Fuzzy Simple Shortest Path Routing Protocol (SF_SSP) for Underwater Communication. Indian Journal of Science and Technology 16(44): 4016-4025. https://doi.org/10.17485/IJST/v16i44.2009

* **Corresponding author**.

salma.jce@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The primary objective of the protocol is to detect malicious nodes accurately and efficiently. Malicious nodes can disrupt communication, drop packets, or launch various attacks on the network. By using fuzzy logic, this protocol considers multiple parameters and behaviors of nodes to identify potential malicious activities. **Methods:** In this work, fuzzy logic rules are utilized for evaluating various parameters and behaviors for nodes. Fuzzy inference system with linguistic variables and fuzzy rules is also established. **Findings:** In UWSN, Security is one of the key points of consideration in implementing the protocol. However current routing protocols have not been designed to defend against security attacks that can degrade the network performance. Since the nodes in UWSN are susceptible to malicious attacks, it is easier for an adversary to operate and to select UWSN channel along with communication nodes. In the UWSN environment, the presence of selfish nodes degrades the performance of the confidence nodes. This presence of selfish nodes in UWSN also leads to connection letdown between communication nodes. In this research work, an intelligent routing technique is introduced to Simple Shortest Path (SSP) routing protocol. We have added fuzzy-based security to SSP that enhances the SSP performance. This research work proposes fuzzy-based selfish node detection and removing those selfish nodes from routing. The parameters which describe the behavior of individual nodes are extracted and evaluated using fuzzy rules. The proposed SF_SSP provides higher throughput and packet Delivery Ratio compared to VBF, and SSP. **Novelty:** The novelty of detecting malicious nodes in underwater communication lies in its adaptive and robust trust evaluation using fuzzy logic to handle uncertainty and dynamic underwater conditions effectively. In this work, we have strengthened the Simple Shortest Path (SSP) routing scheme by adding fuzzy-based security rules.

Keywords: Dynamic routing; Fuzzy Set; Confidence node; Security; Trust Evaluation

1 Introduction

In the current scenario Underwater Wireless Sensor Network (UWSN) based applications are extensively considered for oceanic data collection, oil investigation, pollution tracking and tactical scrutiny, etc. All sensors deployed underwater as in Figure 1 are in three-dimensional scope and the node location normally changes with the topology and the flow of water of Underwater Sensor Networks (USNs) and is more compound than terrestrial Wireless Sensor Networks (WSNs). Routing protocols of terrestrial WSN, which are already deployed are unfit for USN(1). It creates new challenges for intriguing routing protocols for USNs(2). In the context of underwater, acoustic transmission is looked at as an appropriate medium. Nevertheless, due to the sound signal's physical attributes, acoustic passages are prone to low bandwidth availability, large delay in propagation, and high error probability. A holistic authentic transmission is a foremost and onerous issue for designing pacts for Underwater Acoustic Sensor Networks (UASNs). Furthermore, the nodes servicing underwater are equipped with power batteries and are hard to replace.

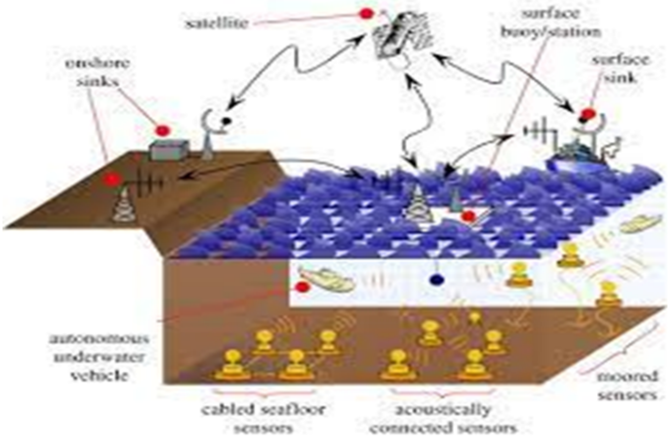

Fig 1. Underwater Communication

SSP is used in underwater communication for several reasons:

1. **Energy Efficiency:** Underwater communication devices, such as underwater sensors and autonomous underwater vehicles (AUVs), often have limited energy resources. Shortest path routing helps minimize the energy consumption of these devices by reducing the distance they need to travel or the number of hops they need to make to reach their destination. This efficiency is crucial for extending the operational lifetime of underwater devices.
2. **Minimizing Latency:** Shortest path routing helps reduce communication delays in underwater networks. In time-sensitive applications like environmental monitoring, disaster response, or underwater robotics, minimizing latency is critical. Shortest path routing minimizes the distance and time it takes for data to traverse the network.
3. **Bandwidth Conservation:** Underwater communication channels can have limited bandwidth, making efficient use of available resources important. Shortest path routing can help avoid unnecessary data transmission through longer routes, preserving bandwidth for other important communication needs.
4. **Simplified Implementation:** Shortest path routing protocols are relatively straightforward to implement and manage. This simplicity can be beneficial in underwater communication networks, which may have constraints on computational resources and real-time decision-making.
5. **Robustness:** Shortest path routing can enhance the robustness of underwater networks. By choosing the shortest path, it reduces the chances of encountering interference, obstacles, or signal degradation that can occur in the underwater environment. This can help maintain network connectivity and reliability.
6. **Adaptability:** Underwater environments can be dynamic and subject to changes, such as the movement of underwater vehicles, ocean currents, and variations in water properties. Shortest path routing protocols can quickly adapt to these changes, ensuring that data is delivered efficiently.

It's worth noting that while shortest path routing is commonly used, there may be situations where other routing algorithms, like geographic routing or quality-of-service (QoS) routing, are more appropriate based on specific underwater communication network requirements and constraints. The choice of routing protocol ultimately depends on the specific goals, network topology, and environmental conditions of the underwater communication application.

Simple Shortest Path routing protocols, while effective for finding the most efficient communication paths in a network, have limitations when it comes to detecting malicious nodes and removing them from the communication path. Some of the limitations include:

1. **Lack of Security Mechanisms:** Simple shortest path routing protocols often lack built-in security mechanisms for detecting and mitigating malicious nodes. They primarily focus on finding the shortest path based on distance or hop count and do not have the capability to identify and respond to security threats.
2. **Limited Authentication:** Many shortest path routing protocols do not provide robust node authentication mechanisms. As a result, malicious nodes can impersonate legitimate nodes and participate in the network, making it challenging to distinguish between authorized and unauthorized devices.
3. **Vulnerability to Spoofing and Attacks:** Malicious nodes can inject false routing information into the network, leading to incorrect path selection. This can result in compromised communication paths, and the routing protocol may not have mechanisms to detect or prevent this kind of interference.
4. **Lack of Intrusion Detection:** Shortest path routing protocols often lack intrusion detection capabilities. They are typically designed for efficiency and simplicity, so they may not incorporate features for monitoring and identifying malicious behavior within the network.
5. **Incomplete Visibility:** Simple shortest path routing protocols may not provide complete visibility into the network, making it difficult to detect and isolate malicious nodes. They may not have the means to collect and analyze network-wide data to identify anomalies or malicious activity.
6. **Limited Adaptability:** These protocols may not adapt well to changes in network conditions or evolving threats. Malicious nodes can change their behavior or location to avoid detection, and simple routing protocols may not be able to respond effectively to these dynamic situations.
7. **Inability to Isolate Malicious Nodes:** Detecting a malicious node is one thing, but removing it from the communication path is another challenge. Simple routing protocols may not have mechanisms for isolating or blocking malicious nodes effectively, leaving the network vulnerable.

To address these limitations, more advanced routing protocols and network security measures should be implemented in underwater communication networks. These may include intrusion detection systems, encryption, secure authentication mechanisms, anomaly detection, and routing protocols that are designed with security as a primary consideration. Additionally, regular network monitoring and maintenance should be conducted to identify and respond to potential threats and compromised nodes.

A vector-based energy-conserved data-directing protocol for UWSNs is introduced in[2]. The nodes situated in the middle decide whether to lead packets or not by contemplating the benefits in line with their location. Due to this, the packet-forwarding node counts are dropped and consequently, the energy expenditure is brought down. The reliability of the packet transmission is increased by heading data packets in interleaved routes. However, only the location factor is attributed to weighing credits of packet forwarding, which results in energy consumption among sensor nodes unevenly and abbreviates network lifespan. Moreover, the data transmission reliability is not assured in the circumstances of thinly distributed network

Further, some MAC solutions[3,4] have been suggested for UASNs. In UASNs, the predetermined MAC protocols like TDMA, FDMA, or CDMA cannot be adopted because of limited bandwidth, high delay in propagation, complexity in lock synchronization, etc. Vector Base Forwarding (VBF) and its enhanced routing protocols[5,6] are devised only for the network layer. In such environments, security in conventional UASNs is not considered. In this work, we have added an intelligent routing method to the Simple Shortest Path (SSP) scheme with fuzzy-based rules, so that it is strengthened against malicious attacks and is more robust.

EEMCCP (Energy Efficient Minimum Cost Cluster Routing Protocol) uses the concept of clusters for routing. The Chaotic Algae Algorithm (CAA) is used to cluster the network. One member node of each cluster is selected to act as the CH (Cluster Head)[7,8]. The EEMCCP scheme uses only a minimum number of nodes for routing the packets. Received Signal Strength Indicator (RSSI) values are used to select the gateway CH nodes. These Gateway nodes propagate the processed data to the Autonomous Underwater Vehicle (AUV) nodes for further transmission to the surface station. The surface station handles parallel communication with the sink nodes underwater. The base station or the surface station uses radio frequency signals to route the data towards the destination[9]. Protocols related to effective routing in wireless sensor ad-hoc networks are always been under research. The routing protocol must incorporate effective and reliable communication as part of its design framework. In fact, routing in UASNs is far more challenging than routing for terrestrial regions. The routing protocols for underwater communication face a lot of limitations and restrictions than on land[10]. The movement of the currents underwater poses a challenge to the moving nodes. Also, the propagation of delay underwater is higher than on land. Additionally, UASN-based technologies are limited in their operations due to the underwater acoustic waves and channels. Most of the time, underwater acoustic sensor networks are expected to function at short notice. In other words, the communication setup needs to be deployed with no prior arrangement underwater. In case of a broken route, the routing protocol must be able to repair it without undue delay[11]. The routing protocol designed for underwater communication must be self-adaptive and robust at all times. The architectural implementation of UASNs has been under constant research to provide effective solutions for UASNs. Various researchers are exploring areas where protocols for routing, MAC layer, link layer, communication, etc., have been studied thoroughly. The principles and characteristics of different protocols were compared regarding important aspects such as clustering and transmission[12]. The protocols were also categorized based on their architecture, data forwarding methods, and related operations[13]. This work also reviewed the protocol design of the underwater acoustic network. The latest research on UASNs has been analyzed by the authors to understand the current challenges and issues in underwater communication[14]. Special attention was given to the MAC layer and network layer as these two need to be well-developed to achieve effective communication[15,16]. As the number of nodes entering the network grows linearly, the network efficiently manages the situation. UWSNs can benefit immensely from implementing a cross-layer design in their protocols. Underwater communication is riddled with a lot of challenges and issues in terms of routing and security. To address these issues, using a cross-layer approach would be much more beneficial in terms of not having to worry about standards and protocols exclusive for each layer. This would offer a lot of freedom to the designed protocols in solving the prevalent issues in underwater communication rather than focusing on addressing the protocol standards for each layer. Due to the limited resources, cross-layer optimization will work effectively in combining the resources of the layers of the OSI model.

Encryption has always been combined with network protocols to ensure secure information[17]. With the help of a secure key, it is possible to transfer data along any type of network. The ciphertext is very secure and is useless without the correct key. Various encryption techniques have been proposed and implemented by several researchers. These techniques are capable of withstanding any type of unauthorized attack. Rivest et. al have studied the scope of performing computational operations on encrypted data without decrypting it. This has posed an open problem in the field of cryptography[18]. Fully Homomorphic Encryption (FHE) allows arbitrary operations on the encrypted data. Researchers have found a way to do multiplication or addition on the encrypted data[19]. Recently, schemes have been proposed to conduct both multiplication and addition on encrypted data. Gentry et al. developed an FHE scheme in 2009. This scheme is capable of supporting both multiplication and addition of operations without any limit to the number of operations that can be committed. Gentry's FHE is not completely efficient but was able to achieve a moderate amount of success. SSP protocol was originally designed with a focus on efficiency and simplicity and security was not a primary consideration. As a result, they lack advanced security features such as intrusion detection, intrusion prevention, and anomaly detection. In SF_SSP fuzzy logic method is used to create rules that define normal behavior for network nodes and traffic patterns. Deviation from these norms can trigger alerts, helping to identify potentially malicious nodes. For example, if a node suddenly starts advertising routes that deviate significantly from its historical behavior, fuzzy logic-based rules can flag this as an anomaly. A cross-layer protocol SF_SSP is proposed in this work that extracts the individual node behaviors, evaluate the nodes, detects and removes the selfish nodes in UWSN. The methodology used to combat selfish nodes based on fuzzy sets is presented. The fuzzy set-based result finds the selfish node and also gives the solution to reduce data loss over a network. SF_SSP can help overcome limitations of SSP related to the security and detection of malicious nodes by providing more adaptive, nuanced, and context-aware decision-making capabilities. This approach can improve the resilience and security of the network while mitigating the vulnerabilities of traditional routing protocols.

2 Methodology

This research work presents a confidence-based SF-SSP model which makes use of the confidence factor to ascertain the most eligible node for the process of data routing. The SF-SSP uses fuzzy rules to estimate the confidence factor of the participating sensor nodes in data transmission underwater. This assertion uses parameters gathered from all the nodes which are part of data forwarding to make suitable decisions along with controlling unreliability to bring out the most acceptable output. The confidence factor is not accepted as probabilities but rather results as human decision entities like less, more, etc. The flowchart of the proposed protocol is shown in Figure 2.

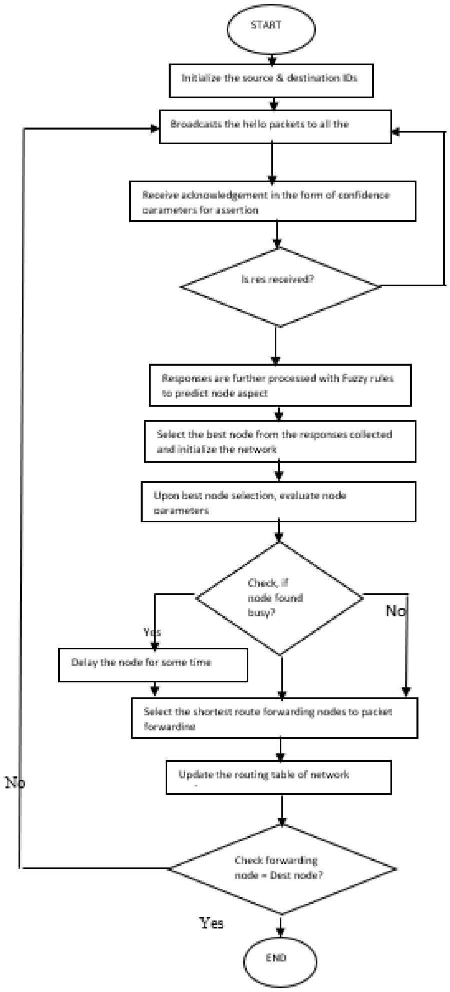
START
Initialize the source & destination IDs
Broadcasts the hello packets to all the
Receive acknowledgement in the form of confidence parameters for assertion
Is res received?
Responses are further processed with Fuzzy rules to predict node aspect
Select the best node from the responses collected and initialize the network
Upon best node selection, evaluate node parameters
Check, if node found busy?
Yes
No
Delay the node for some time
Select the shortest route forwarding nodes to packet forwarding
Update the routing table of network
No
Check forwarding node = Dest node?
Yes
END

Fig 2. Flowchart of SF_SSP

2.1 SF_SSP using confidence

Here the data underwater is obtained from nodes in the underlying layers underwater ensuring secure data movement among sensors deployed underwater using the confidence factor. The protocol design is formed using confidence concept (M) as in eq.1. Confidence concept is the assertion initiation parameter (Ai) incorporated with confidence factor (C) among all the sensor nodes underwater. The entire plan of action is formulated in eq.2.

$$M = A_i \ \oplus \ C \tag{1}$$

A_i is available as a frizzy value apart from binary value. In addition, φ is Signal to Noise Ratio (SNR) that determines broadcast of control signals, r denotes (rate of data packets relayed) the time taken to collect the data packets from broadcast, B is the buffer memory occupation span and E indicates node residual energy underwater. Initially, Confidence factor (C) is iterated as packets start routing and is framed in subsequent eq. 3 and eq.4. Moreover, σ_r represents successful data transmission rate, the fairplay ratio γ is best path selection parameter and τ be the data transfer duration. The thresholds are correlated with the set of variables regarded as dissimilarities in eq. 2 and 3. These parameters ensure the ability of the protocol along with confidence factors to limit the effect of security offences with no comptonization in the communication reliability. The node prominence is marked as confident if $(C \ \geq \ C^{threshold})$, unsure (if $(C^{minimum} \ \leq C \ < \ C^{threshold})$ and unconfident if it goes below threshold. This confidence calculation uses the fuzzy logic confidence estimation process in order to obtain the confidence value. The confidence factor of every node is similar if observed directly using this framework. The eq. 4 formulates the confidence (C_a^b) of node a to node b considering radio signal range as network with data forwarding rate (ρ) and volume (π) as a function(f)

$$A_i \begin{cases} node_{fully_{accepted}},\, if \begin{cases} \varphi \geq \varphi^{threshold} \\ r \leq r^{threshold} \\ B \leq B^{threshold} \\ E_{residual} \geq E_{residual}^{threshold} \\ \delta \geq \delta^{threshold} \end{cases} \\ node\_marginally\_accepted,\, if \begin{cases} \varphi^{minimum} \leq \varphi < \varphi^{threshold} \\ r^{mininum} \leq r < r^{threshold} \\ B^{threshold} < B \leq B^{maximum} \\ E_{residual}^{minimum} \leq E_{residual} < E_{residual}^{threshold} \\ \delta^{minimum} \leq \delta < \delta^{threshold} \end{cases} \\ node\_not\_accepted,\ if\ otherwise \end{cases}$$

Fig 3. Equation 2

parameters. Parameter f is a Bayesian function of data drip and false packet introduction underwater. Parameter ρ is data drip by node A and B & it occurs in underlined conditions:

- Packets sent from A but remain unnoticed by B
- Due to heavy congestion, the overall packets avoided by node B
- Data forwarding delay by B

The parameter π is the packets originated from untrusty nodes having the constraints mentioned below:

- Packets wrongly routed by node A
- Packets are uncertainly inhibited by node A

$$A_i \begin{cases} confident\_node,\ if \begin{cases} \sigma_r \geq \sigma_r^{threshold} \\ \gamma_r \leq \gamma_r^{threshold} \\ \tau \leq \tau^{threshold} \end{cases} \\ unsure\_node,\ if \begin{cases} \sigma_r^{minimum} \leq \sigma_r < \sigma_r^{threshold} \\ \gamma_r^{threshold} \leq \gamma_r < \gamma_r^{maximum} \\ \tau^{threshold} \leq \tau < \tau^{maximum} \end{cases} \\ not\_confident\_node,\ if\ Otherwise \end{cases}$$

Fig 4. Equation 3

The above constraints are presented as functions same as traffic and volume parameters which are necessary to find confidence factors that allow the operations of sensor nodes layer-wise.

$$C_a^b = f(\rho, \pi) \tag{4}$$

2.2 SF_SSP using Fuzzy Logic confidence

It is incorporated in acquiring phase which is the assertion initiation phase for eligible nodes and the packet forwarding phase; it is a confidence between eligible nodes. This framework is designed to securely select sensor nodes for data routing and forwarding to the destination.

2.3 Network Acquiring Phase

It is a phase when node A broadcasts the control or beacon packets to all the other nodes in the network with locations of source node A and destination node B. Upon receiving control signals from node, A, the nodes participating in the routing process reply to A with the acknowledgment. Confidence factors for all the acknowledged nodes will be calculated and upgraded using frizzy rules to notify the appropriateness of the participating nodes like fully accepted, marginally accepted or not accepted. The node with highest confidence is given highest priority by fuzzy rules.

2.4 Data Forwarding Phase

Upon best node selection on the confidence factor, the data forwarding process begins by following the shortest route path to destination. Packets get routed from the source to forwarding nodes and finally reach to receiver node. Parameters like data forwarding success ratio (Sr); it decides the data reliability, transfer duration (δ); it is a time elapsed in data packet originated from sender to duration of number of packets transmitted within that timestamp and fair play ratio (γ); elects the node for relay in next distance between the neighbor nodes. If a node selected for data forwarding and found busy is delayed for certain period by decreasing it's γ and δ values to assure node isolation for further processes to avoid untrusty activity.

3 Results and Discussion

This section presents the performance of the proposed routing scheme SF_SSP by simulation trials. Simulation is done using MATLAB. In an area of 100m * 100m, hundred sensor nodes are deployed. In this work, we have added intelligence to the SSP (Simple Shortest Path) routing scheme. To the best of our information, the proposed fuzzy set-based SF_SSP is the first fuzzy-based secure shortest path protocol for UWSN. The above-mentioned secure routing protocol does not use asymmetric encryption and decryption processes. The presented fuzzy-based secure routing scheme is based on node identity. The sender node does not have to apply for the public key of the destination node, which evades extra delay, bandwidth, energy, propagation delay, and narrow bandwidth.

Furthermore, we conducted a number of experiments to compare the performance of the proposed scheme with the existing underwater protocols in terms of energy consumption, throughput, and packet delivery rate.

The simulation analysis is carried out here for the implemented confidence model, which has the ability to resist various malicious offenses compared to VBF and SSP protocols. The computation of confidence value decides how trusty the node is, so that it can be included for optimal path routing which enhances the performance of the presented protocol. The packet loss rate is the deciding parameter in the case of network intrusion tolerance. The idea is to minimize the packet loss and is accomplished by selecting the node with a high confidence value so that the packets can be delivered to the destination effectively. The proposed model yields a minimum rate of packet loss as compared to VBF & SSP protocols. From Figure 5 it is seen that as the node count increases throughput also increases for all the three protocols, and the throughput of the proposed method is higher than VBF, and SSP.

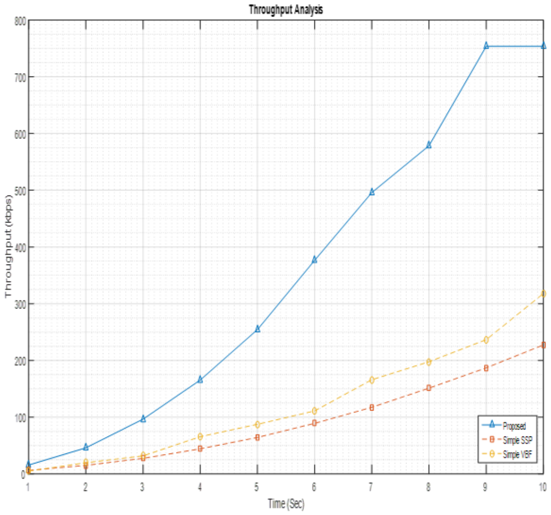

Fig 5. Throughput of proposed and VBF, SSP

The energy efficiency analysis of the existing and implemented protocol is shown in Figure 6 . The energy consumption increases due to the incurrence of malicious nodes in the network, packet handover process, and packet losses due to attacks posed by intruders. From Figure 6 it can be seen as the node count increases energy also increases for all three protocols, the total energy in the projected procedure is to some extent higher than VBF, and SSP which is reasonable.

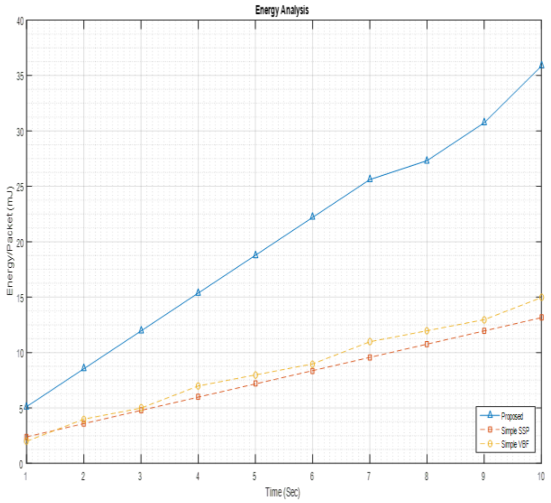

Fig 6. Energy of proposed and VBF, SSP

The node behaviors cannot be monitored by VBF & SSP because they have no security mechanisms like the proposed model. Hence there exists much packet loss as compared to the proposed model. Due to the rejection of malicious nodes, the packet loss rate can be thoroughly minimized.

The packet delivery rate increases with the number of nodes with three routing protocols as shown in Figure 7 When the number of nodes is increased to 100 SF_SSP achieves the highest packet delivery rate. The Figure 7 depicts the comparative result between the methodology implemented in this research work with the protocols that already exist. As the route establishment is secure because of the election of confident nodes for the optimal path routing by ejecting the intruding nodes, the packet transfer rate is improved yielding to highest throughput as compared to VBF & SSP protocols.

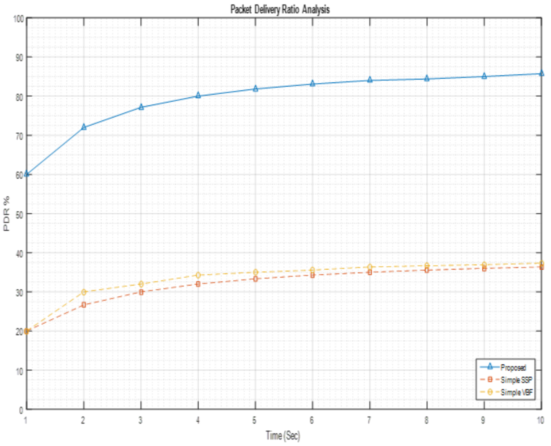

Fig 7. PDR of proposed and VBF,SSP

The Figure 8 shows analysis of route distance for the proposed protocol with the protocols that already exist. The proposed model yields lower route distance since it selects the nodes which are highly trustworthy and passes the packets through the shortest path to the destination. Also, the proposed model has the potential to reject malicious nodes by ejecting the falsy responses received during the control signal flooding phase and enables the most efficient and secured routing to the destination. This model consumes time in selecting confident node by ejecting malicious nodes for secure routing as compared to other two conventional protocols such as VBF & and SSP.

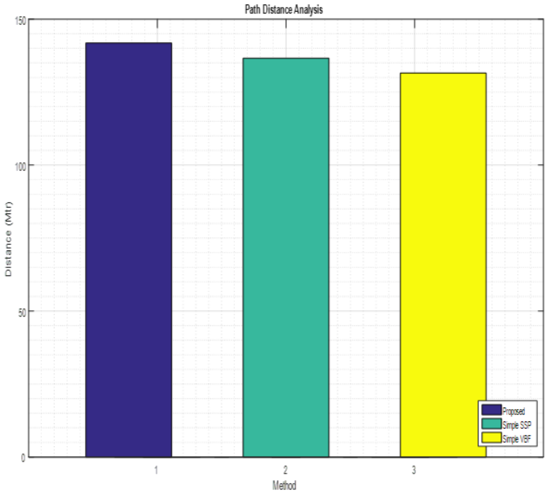

Fig 8. Path DistanceAnalysis of proposed and VBF, SSP

4 Conclusion

In UWSN, the network security can be improved by the implementation of the proposed model. It yields better results with respect to rejecting malicious nodes of the network, minimizing packet losses by allowing secured routing to the destination because it uses only trusty nodes for the routing based on confidence value pertaining to every intermittent node that are part of control signal flooding phase. Shortest path routing protocols, when integrated with fuzzy rule-based systems for detecting malicious nodes, enhance network security by providing a dynamic and adaptable approach to identifying and isolating potential threats based on rule-defined criteria. The implemented model is considered as a secured protocol as compared to VBF & SSP. The comparative evaluation is carried out by contemplating parameters like route distance, packet loss rate, throughput and energy consumption. The proposed protocol gives better results compared to other two conventional protocols. The proposed methodology stated in this work achieves 46% more PDR then SSP, VBF, 85% more throughput then SSP, 95% more then VBF for the presence of 100 number of nodes. The proposed protocol shows an improvement over the existing SSP, VBF protocol.

References

1) Hu Y, Chen L, Sun Y. The Cooperative-Communication Based Underwater Layered Routing Protocol for Underwater Wireless Sensor Network. *Wireless Personal Communications*. 2022;125(4):3019–3047. Available from: https://doi.org/10.1007/s11277-022-09696-w.
2) Kumar PJS, Ponnusamy M, Radhik R, Dhurgadevi M. Underwater clustering based hybrid routing protocol using fuzzy ELM and hybrid ABC techniques. *Journal of Intelligent & Fuzzy Systems*. 2023;45(1):831–843. Available from: https://doi.org/10.3233/jifs-230172.
3) Mittal A, Correa FS. Adaptive Fuzzy Optimized Routing based on Maximum Energy Support Routing Protocol using Synchronized SleepModel Routing Algorithm for WSN. *2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*. 2023. Available from: https://doi.org/10.1109/icdcece57866.2023.10151019.
4) Han D, Du X, Liu X, Tian X. FCLR: Fuzzy Control-Based Layering Routing Protocol for Underwater Acoustic Networks. *IEEE Sensors Journal*. 2022;22(23):23590–23602. Available from: https://doi.org/10.1109/jsen.2022.3218136.
5) Kumar A. A new optimized least-square sparse channel estimation scheme for underwater acoustic communication. *International Journal of Communication Systems*. 2023;36(6). Available from: https://doi.org/10.1002/dac.5436.
6) Xu H, Shi W, Sun Y. Performance analysis and design of quasi-cyclic LDPC codes for underwater magnetic induction communications. *Physical Communication*. 2023;56:101950. Available from: https://doi.org/10.1016/j.phycom.2022.101950.
7) Sabbagh AG. Long-range underwater optical wireless communication systems in turbulent conditions. *Optics Express*. 2023;31(13):21311. Available from: https://doi.org/10.1364/oe.489759.
8) Ali F, Jayakody M, N D. SIMO-Underwater Visible Light Communication (UVLC) system. *Computer Networks*. 2023;232:109750. Available from: https://doi.org/10.1016/j.comnet.2023.109750.
9) Sun K, Han B, Yang J, Li B, Zhang B, Liu K, et al. Study on the Influence of Underwater LED Illumination on Bidirectional Underwater Wireless Optical Communication. *Photonics*. 2023;10(5):596. Available from: https://doi.org/10.3390/photonics10050596.
10) Zhu Z, Zhou Y, Wang R, Tong F. Internet of Underwater Things Infrastructure: A Shared Underwater Acoustic Communication Layer Scheme for Real-world Underwater Acoustic Experiments. *IEEE Transactions on Aerospace and Electronic Systems*. 2023;p. 1–14. Available from: https://doi.org/10.1109/taes.2023.3281531.

11) M SV. Underwater Image Enhancement. *International Journal of Advanced Research in Computer and Communication Engineering*. 2023;12(3). Available from: https://doi.org/10.17148/ijarcce.2023.12330.

12) More S, Bartakke P, Aggrawal M. Multipath Modeling under Tank Environment for Underwater Acoustic Communication. *2021 Advanced Communication Technologies and Signal Processing (ACTS)*. 2021. Available from: https://doi.org/10.1109/acts53447.2021.9708257.

13) Ma H, Teng J, Hu T, Shi P, Wang S. Co-communication Protocol of Underwater Sensor Networks with Quantum and Acoustic Communication Capabilities. *Wireless Personal Communications*. 2020;113(1):337–347. Available from: https://doi.org/10.1007/s11277-020-07192-7.

14) Kida Y, Deguchi M, Watanabe Y, Shimura T. Experiments for long-range high-rate underwater acoustic MIMO communication using adaptive passive time reversal. *2023 IEEE Underwater Technology (UT)*. 2023. Available from: https://doi.org/10.1109/ut49729.2023.10103409.

15) Zhang Y, Chang J, Liu Y, Xing L, Shen X. Deep learning and expert knowledge based underwater acoustic OFDM receiver. *Physical Communication*. 2023;58:102041. Available from: https://doi.org/10.1016/j.phycom.2023.102041.

16) Prasad SKR, Gurugopinath S. Deep Learning Techniques for Detection of Underwater Acoustic Sources. *2023 11th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON)*. 2023. Available from: https://doi.org/10.1109/iemecon56962.2023.10092324.

17) Wei Y, Quan L, Xu W, Wang D, Wang L. An In-Phase/Quadrature Index Modulation-Aided Spread Spectrum Communication System for Underwater Acoustic Communication. *Electronics*. 2023;12(13):2919. Available from: https://doi.org/10.3390/electronics12132919.

18) Madhu R, Kumar MNVSS, Umamaheswararao S. Wireless underwater channel modelling for acoustic communication. *International Journal of Computational Vision and Robotics*. 2023;1(1):1. Available from: https://doi.org/10.1504/ijcvr.2023.10054629.

19) Lidstrom V. Polar Coded Non-Coherent Acoustic Underwater Communication. *2021 Fifth Underwater Communications and Networking Conference (UComms)*. 2021. Available from: https://doi.org/10.1109/ucomms50339.2021.9598134.