TRSOR: TRUSTWORTHY ROUTE SELECTION AND OPPORTUNISTIC ROUTING FOR UNDERWATER WIRELESS SENSOR NETWORKS

S. P. Saranya[1], **S. Chitra**[2]

Abstract

Underwater wireless sensor networks (UWSN)s are unique from terrestrial networks in several ways. This includes a restricted supply of energy, a lower bandwidth, longer propagation latencies, a more dynamic topology, and a higher error rate. For this reason, opportunistic Routing has recently attracted a lot of attention to improve packets' delivery rate and the energy efficiency of UWSNs in such a setting. Cooperating sensors in the ocean may use opportunistic data routing to send a packet to its destination, which is a good strategy for overcoming channel impairments like packet loss. This article presents a new routing protocol, the trustworthy route selection and opportunistic Routing protocol (TRSOR), that addresses the void issue and the high bit error rate without requiring a global positioning system. TRSOR can effectively and at the lowest feasible cost (including energy and latency) bypass all sorts of vacant spaces while picking the set of candidate nodes with the greatest packet progress. By altering the size of its forwarding set in response to the density of its neighbors, a forwarding node may strike a balance between packet throughput and energy consumption (sparse or dense). As a bonus, TRSOR may choose the forwarding set in any direction away from the sender (barring any hidden nodes). In a comprehensive simulation study, we found that TRSOR has much better results than other protocols regarding packet delivery ratio, energy consumption, and average end-to-end latency.

KeyWords: TRSOR, Trust, UWSN, opportunistic Routing, Route Selection.

DOI Number: 10.14704/nq.2022.20.8.NQ44711 **NeuroQuantology 2022; 20(8): 6850-6859**

---

[1] Ph.D. Research Scholar, PG & Research Department of Computer Science, Government Arts College (Autonomous), Coimbatore

[2] Ph.D., Associate Professor, PG & Research Department of Computer Science, Government Arts College(Autonomous), Coimbatore

Introduction

Recent years have seen a surge in interest in UWSNs [1-3] from the wireless communication and networking communities. Offshore exploration, ocean monitoring, research on marine and animal life, and regulating mineral extraction from the deep water are just some of the many uses for UWSNs. Underwater sensor nodes collect environmental data and send it to sonobuoys on the surface, which then send it to a data center for processing [4].

Nonetheless, the sensor is exclusively used to perform sensing duties and transmits important data to actors. Like the sink, actors monitor the whole system and use data from sensors to guide their actions. Sometimes the spot/void hole is farther from a dying or soon-to-die state than the state when relevant nodes are not active. To use a jargony term, the problem with these voids is called the Hotspot Problem [2-5]. A network comprising sensor and actor nodes and some gateway nodes is the optimal solution for partitioning a network into a cluster or other division, such as subnets in the ocean (that serve a required function within the Network).[6].

Since the nodes rely mostly on battery power, there are constraints on how much power may be used given the extreme and typically subterranean conditions [7]. It takes more energy to underwater power sensors than on land ones because of the necessity for sonic waves for transmission. Therefore, a reliable routing system is essential for keeping the Network operational for as long as possible [9, 10].

Opportunistic Routing is an effective method in sensor networks because of its potential to improve transmission reliability and network performance. This is how packet forwarding is made possible: when the neighbors of a node all receive a packet at the same time and contribute to transmitting it, the node may move on to the next hop in the Network [11]. However, an opportunistic routing strategy developed for terrestrial networks is unlikely to be effective when applied to UWSNs. Error bit rate, energy use, node mobility, and sluggish propagation speed all impact the priority and selection of forwarding sets in an underwater environment. Additionally, several opportunistic terrestrial techniques are GPS-based, making them incompatible with underwater situations where GPS is unavailable [16-20].

This research aims to offer a new Trustworthy Route Selection and Opportunistic Routing (TRSOR) protocol for improving performance and reliability in lossy and sparse underwater settings. TRSOR's approach to sparse and loss settings imposes far less overhead than protocols that rely on expensive localization to derive geographic coordinates in underwater environments. Furthermore, TRSOR does not depend on global topological information as other shameful protocols do; instead, it uses information provided by nodes just one hop away. Information from the sink node's distributed beaconing mechanism is used by each forwarding node to identify its forwarding set.

TRSOR could pick a collection of candidate nodes that makes the maximum progress toward the sink while avoiding void nodes so that it doesn't become trapped there. When the forwarding set is determined, it allows the forwarding nodes to work together to prevent excessive traffic and save energy by halting communications that aren't essential. A high-density forwarding set's energy usage may be reduced by appropriately changing the number of receiving nodes.

Based on the simulation findings, we know that our method improves the delivery rate of each sent packet and inherently discards routes that go to the area of interest.

Section III suggests a methodology, and Section IV examines simulation and performance analysis, rounding out the study's organization. In the fifth section, we draw our conclusions.

BACKGROUND STUDY

S. Basagni et al. [2] demonstrated the efficiency of CARP as a novel technique for UWSNs. By sending short control messages, CARP efficiently implements joint channel access and relay selection, as the cross-layer design paradigm requires. The well-known technique is augmented by the Channel-aware Routing Protocol (CARP), which incorporates information about the connection quality into the cross-layer relay selection process. The chosen link's robustness is also determined by estimating the transmission power required to produce a comparable packet error rate for short control and larger data packets. The brief control packet exchange finds connections that result in reliable data transfers.

Coutinho, R. W. L. et al. [3] To enhance the efficacy of data transmission in UWSNs, the GEographic and opportunistic routing protocol with Depth Adjustment-based topology management for communication Recovery across void areas (GEDAR) was developed and tested. Based on the positions of the nodes and the broadcast communication channel, GEDAR distributes data packets opportunistically to sonobuoys floating on the ocean's surface. GEDAR employs a novel depth adjustment-based topology management method to fill communication gaps that move void nodes to different depths.

U. Draz et al. [6] There is a basic challenge in forwarding data packets to the sink when Sink Neighboring Nodes (SNN) have died or are soon to die. This article proposes a solution to the problem mentioned above in UWSNs by assigning watchman nodes to the 71 percent of the Earth that is not currently being monitored. The issue is now solved using the new watchman-based data packet forwarding method.

S. M. Ghoreyshi et al. [8] opportunistic routing in UWSNs was investigated for its ability to facilitate the shortcomings of acoustic transmission by enlisting intermediary nodes to relay packets. To minimize packet loss and maximize transmission reliability in very noisy and fading channels, the opportunistic void avoidance routing (OVAR) technique is suggested. Contiguous clusters are established by eliminating the possibility of hidden nodes in each cluster, and the optimum forwarding set is chosen.

S. Karim et al. [12] Define the term "Geographic and Cooperative Opportunistic Routing," which you used to describe a revolutionary routing protocol you developed (GCORP). After gathering depth information from nearby nodes, the source node computed a fitness factor to choose a forwarding set of relay nodes. The surface sink node started a depth measurement by sending a distributed beacon message. Afterward, the optimal relay forwarding configuration was selected at the source node using a weighted approach. Normalized energy, power dissipation potential, and distance at each relay node were all subjected to the weight calculation method.

A. Khan et al. [13] UWSNs have been researched for energy-efficient packet transfer from source to destination. Because underwater communication requires a limited amount of battery power from the nodes, the study objective was to decrease the nodes' energy usage. This piece presented a low-power routing system, resilient to interference and aware of its potential routes (EEIRA). Direct and optimum relay data transmission from source to destination is a feature of this method.

Tonghong Li. [17], When establishing UWSNs, the authors recommend a tiered architecture in which an acoustic mesh network serves as the "backbone network" for sensor nodes connecting the UWSNs to the centralized monitoring system. The authors propose a practical routing strategy for a mesh network deployed in the water. Within a particular belt, our best-effort protocol is sent via many independently routed channels. With "multi-sink routing," the authors can increase packet delivery rates by sending data from a single source node to several sinks located in different parts of the world at the same time via a variety of different paths.

Zhou, Z. et al. [20] There must be a routing mechanism that minimizes wasted energy and data traffic. In this research, we provide E-CARP, a refined form of the Channel-Aware Routing Protocol (CARP) designed to solve this issue.

PROBLEM STATEMENT

The recommended CARP uses a randomized routing architecture built on bogus packets to prevent an eavesdropper from discovering the source or sink nodes. Because the protocol randomizes the routing path, an attacker cannot use it to pinpoint a node's position in the Network, whether the sender or the recipient. With CARP, nodes may maintain separate lists of nearby and faraway neighbors. The list is generated using the node's geographic information or a technique for counting and exchanging hops. The foreground and background anomaly scores and their respective references are then used as input parameters of the trained ANFIS model to derive the real-time danger level. The current user's risk level, as determined by the decision module, is. To remedy this issue, the authors inject fake packets into the traffic stream to level the playing field. Subsequently, listed nodes get forged packets.

Let's suppose an adversary places a rogue node in the Network, and that node ends up on the created list since consensus includes it. The attacker will likely ramp up their attacks, making the security mechanism useless. To deal with aggressive or hacked nodes, we devised a trust management method that allows each node to assess the trustworthiness of other nodes. Using this metric, nodes will choose a neighboring node from which to send data packets.

PROPOSED MODEL

Sparsely distributed UW-sensor nodes in the Network provide data on underwater ecosystems. In most cases, the Base Station (BS) just sends brief pieces of control information out to the UWSN nodes. For packet security and low power consumption, UWASNs need a block cipher design. The conceptual system model of the suggested approach is shown in Figure 1. To assemble the cluster and pick CH, as proposed in our previous work[7].

SNs operate as secure trust managers in UWSNs to reduce energy usage. Each SN (Sensor Node) distributes the message to the cluster's members. Additionally, each SN may execute the following functions: (1) All cluster members register with their cluster when the action is joined. The corresponding SN can communicate with the rest of the cluster. (2) SN enables the member to deregister from the cluster during the departing operation. After the cluster members approve the registration process, all cluster members are subjected to a security check using the procedure described in 2. (3). In this case, the SN serves as the security trust manager. SN communicates with the BS through the underwater modem the aggregate message of all cluster members to save energy and resources.

a) NETWORK DESIGN:

Multiple sinks, each talking to a relay and an anchor node, make up the UWSN architecture used in TRSOR. Surface-mounted radio and acoustic modems connect nodes at the sink and the destination. Optimal weight estimates help reduce power consumption in the Network's shallower depth sensor nodes.

The weight function is utilized to strengthen the stability of the Network by providing a method for reducing attenuation losses and noise in shallower areas. Those involved in this process collect data from the satellite's relay nodes and forward it to the offshore stations. Wireless communication between sink nodes is possible. Once a packet arrives at the sink node and can be accessed by other sinks or distant hubs through radio connections, it has been delivered. Relay nodes from different manufacturers dot the water's surface. These nodes' job is to identify packets sent from anchor nodes, then pass them on to their destinations.

Installed on the ocean floor, these nodes (also called source nodes) are limited to sensing and collecting data. Relay nodes facilitate communication between anchor nodes and their final destination. Relay and anchor nodes use sonic waves to talk to sink nodes above the sea.

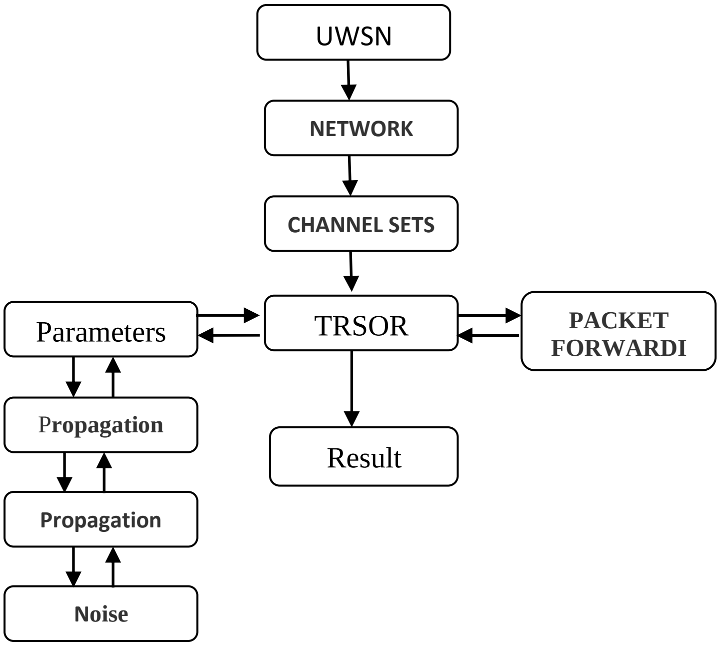

Figure 1: TRSOR Architecture

b) TRSOR:

Some depth-based routing protocols work on a one-hop basis, while others work on a two-hop basis to improve system resilience. To ensure dependability, it is necessary to consider the depth of the next two hops. It is impossible to reduce packet duplication and collisions at the receiving end with these protocols since they cannot increase the time interval between neighboring hops. To improve the efficiency of current routing strategies, we propose a new protocol for UWSNs called Trustworthy Route Selection and Opportunistic Routing (TRSOR). TRSOR sets holding periods for forwarders.

1. The suggested approach enhances the value of priority data forwarding exponentially in exchange for a slight reduction in the depth of the forwarders. Thus, when TRSOR is utilized as a routing strategy for UWSNs, the distant nodes in the transmission may be effectively suppressed.
2. The forwarder is chosen based on forwarding cluster area information from a cluster region with a higher average energy consumption of forwarders to boost network resilience.
3. The shortest route to the sink is computed for each forwarder.
4. Experiments are conducted at various node densities, and transmission ranges to validate TRSOR's performance in various settings.
5. Both with and without data sinks, TRSOR is examined.

c) Link trust

It is possible to model connection behavior using concepts like packet loss, packet error, noise, and interference. Packet loss or transmission errors may occur due to the subpar quality of the underwater connection, and the aquatic environment may undergo fast shifts. The normally benign link may be capable of vicious behavior. As a result, it would be unfair to penalize a lawful node solely for its actions if it were experiencing packet loss or receiving erroneous packets due to a subpar network connection. Concerns are raised if the node doing the monitoring notices anything out of the ordinary happening at the watched node. If packets are lost or corrupted at a greater rate than usual, or if a node's energy consumption is higher than usual, these might be signs of a malicious node in the Network. This is thus because the energy consumption of a node has nothing to do with the behavior of connections. We may describe the connectivity of the underwater cable as,

$L=2-PLR-PER+n(t)+I(t)$------(1)

d) Node Trust

The CH will keep track of each node's trustworthiness and recommend it to a new cluster based on that information. We will use three trust measures for our suggested approach to determine a node's trustworthiness. As defined in [11], Those metrics include the Energy Consumption Rate, the Packet Error Rate, and the Packet Loss Rate (ECR). Loss of packets may occur if the connection's quality is low, as explained in the preceding section on link reliability. However, a compromised or malicious node may wilfully discard packets, alter incoming packets, add bogus information, and reroute them to another node. As a result, the following node will get the incorrect packet.

$T_{pq}=T_q^{PLR}+T_q^{PER}+T_q^{ECR}$------(2)

In this equation, p represents the monitoring node, and q is the monitored node. Trust may be measured via interactions both directly and indirectly.

e) DATA PROPAGATION:

Data speed: It has been shown that at a given depth and salinity, the speed of the acoustic signal increases with increasing temperature and vice versa.

Data is insufficient: Path loss is the primary factor affecting acoustic transmission. As a result, the signal quality in UWSNs degrades. The underwater channel route loss is measured in terms of distance and frequency. The first word denotes spreading loss on the right, whereas the second denotes absorption loss.

Coefficient of data reception: Absorption causes attenuation by transforming the acoustic signal's energy into heat. Frequency affects the degree of attenuation, with higher frequencies requiring more absorption.

Data noise: Underwater communication faces two distinct forms of interference: natural background noise and artificial sounds. Ambient noise is Gaussian in nature, with a constant power spectral density. There are four major sources of ambient noise: Thermal noise, noise caused by waves, noise caused by ships, and turbulence noise.

f) Shortest path Routing Algorithm

Step 1: Set up a wireless network with a single Server node "S," two "Sink" nodes to represent two "Cluster" nodes ("Sink1" and "Sink2"), and an "N"-thousand "Sensor" node array located deep below the surface of

Step 2: Select nodes S (the origin) and D (the destination), where D is either Sink1 or Sink2. Then, invoke the procedure for collecting knowledge

Step 3: Link the nodes in your deployment using sockets.

Step 4: All network nodes will have an energy value of 100 Jules (E), and each trust value will have a value of 10 Jules (T).

Step 5: UWSN call packet forwarding requires the construction of a Routing Table, which serves as a one-hop neighbor for all deployed nodes

Step 6: Make a Route to a Node (i=0, i=n). Assign the node to route table Rt if energy > threshold and trust > threshold. The Right-Handed Returning Step

7: Use the above-deduced router to initiate packet delivery

Step 8: With multi-hop routing mode, a packet may be sent from the source to the destination through many intermediate nodes.

g) Packet forwarding algorithm

First, the inputs consist of the source node, the destination node, and the coverage region.

A node's routing table is obtained.

The Network's nodes will receive a radio signal from the source.

Number four: the origin node discovers its neighbors

It turns out there are new neighbors.

A process should be terminated if the neighboring nodes are the final destination.

A source node's neighbors are considered individually. Individual curiosity and exploration lead to the discovery of the path.

The hop count, RE, and direction matrix are found if the neighbors have no final destination

Verify the size of the degree package.

You may transmit the packets, and the paths have been stored.

Locate the node with the most residual energy, lowest hop count, and final destination.

Search for the nodes experiencing frequent but transient disruptions in connection and high bit error rates

Disconnect the node with the high bit error.

Data flow

h) Knowledge acquirement Algorithm:

step1: broadcasting data discovery message

step2: pick up the data-discovery signals from its neighbors.

step3: Produce a directory of nearby voices and sights.

step4: calculate its hop count and link score value

step5: broadcast its hop count and link score value to its neighbors

step6: receive hop count and link score values from neighbors

step7: if its value is the highest among its optical neighbors

step8: go to a cluster head

step9: else

step10: visit a cluster participant

step11: connect to the neighbor with the highest score.

step12: communicate whether or not it is a cluster head

i) The Probability of Trustworthy:

Assume that the node has a coverage area of volume $V=2\pi R^3/3$ where R is the node's transmission range and denotes this probability as Pb(m). When referring to a node's coverage area near the water's surface, the term "volume" (V) indicates the total amount of space that may be covered. All the space covered by the UWSN in the studied region is virtually divided into tiny cubes. Each cube has a binomial chance of being either filled with one node or empty. If the cubes are sufficiently large, the binomial distribution may be approximated by the Poisson distribution. The probability that m nodes will fill volume V, the top section of the node coverage area.

$$\mathrm{Pb}(m) = \frac{(f_v \sigma dv)^m}{m!} exp\text{--------}(3)$$

Where is the node density in volume? The integral over a given volume, denoted by f v, is equal to v when the density of sensors is distributed uniformly throughout that volume.

In this way, we may calculate the likelihood that a particular node is a "void node," meaning it has no neighbors within the given vertices (V).

$$Pb_v = exp^{-\sigma v}\text{---------------}(4)$$

The likelihood of a void occurring is proportional to (-) and (V). If any of these values (node density or node coverage) drops, void incidence rises.

RESULTS AND DISCUSSION

We make it possible for the mobile sink to go to these potentially hazardous areas to capture the increased data output by the nodes. The local sinks in the area will collect the packets since they do not need to travel farther to reach the surface sinks. Therefore, mobile sinks may provide packets at a low cost, i.e., less energy, leading to a lower energy tax. Since packets encounter void holes more often in sparse UWSNs, those that take several hops to reach the surface sink are more likely to be lost. However, the issue is much reduced in the mobile sink case since the sink moves to other nodes with heavy traffic and collects more data. This tactic increases PDR since it leads to several successful deliveries. Increasing the data rate reduces the probability of collision and increases the number of successfully delivered packets since the time it takes for a packet to reach its destination lowers. For ever-increasing data rates, the linear relationship between PDR and data rate breaks down due to the finite bandwidth of the acoustic transmission. The PDR will be capped once it reaches a certain level.

4.1. Performance metrics

1:The following key performance indicators are monitored to evaluate the Network's security, efficacy, and reliability. To begin, it is possible to define the detection of harmful nodes as the ratio of malicious nodes found to the total number of injected malicious nodes.

2. Power utilization describes how much electricity each node in a network uses to send and receive data.

3. Success in receiving data packets, as a percentage of total data packets delivered, is measured by the Packet Delivery Ratio (PDR).

4.2 Simulation Results

Using the NS2 simulator, we test our suggested protocol. We evaluate the performance of the Weighted Depth and Forwarding Area Division Depth Based Routing (WDFAD) technique and the Enhanced-channel Aware Routing Protocol (E-CARP) against our TRSOR Model. To put the Network's dimensions in perspective, they are 550 m by 480 m.

Opportunistic Routing in the TRSOR approach is based on several factors, such as the energy of the current forwarder and the average energy in the next expected forwarding region, the Shortest Path Index (SPi), which is based on multiple hops to the sink and the average Depth of neighbors in the next expected hop, and the TRSOR algorithm's default Forwarding Policy. To improve the packet delivery ratio and resolve the void hole problem (PDR).

Table 1: Simulation Parameters

Parameters	Value
Simulation Time	900(s)
Number of Nodes	0 to 102
Data Rate	1Mbps
Routing Protocol	GPSR
Bandwidth	2 Mb
Simulation Area	1300 x 2250 m
Transmission Range	250m
Threshold	100dbm
MAC	802.11

Power monitor threshold	120dbm

Packet Size	Throughput			Energy			Time			Packet Delivery ratio		
In MBs	WDFAD	E-CARP	TRSOR	WDFAD	E-CARP	TRSOR	E-CARP	WDFAD	TRSOR	E-CARP	WDFAD	TRSOR
5	991	989	990	21	25	19	1200	1250	1190	1800	1700	1900
10	980	988	991	21	24	19	1430	1450	1330	2899	2500	3000
15	984	991	992	25	27	20	2430	2500	2360	2955	2800	3010
20	990	995	997	25	29	21	2943	3000	2530	2976	2850	3145
25	996	998	999	28	30	22	3135	3200	3100	3023	2950	3250
30	995	999	1020	29	31	23	3425	3450	3101	3212	3101	3312

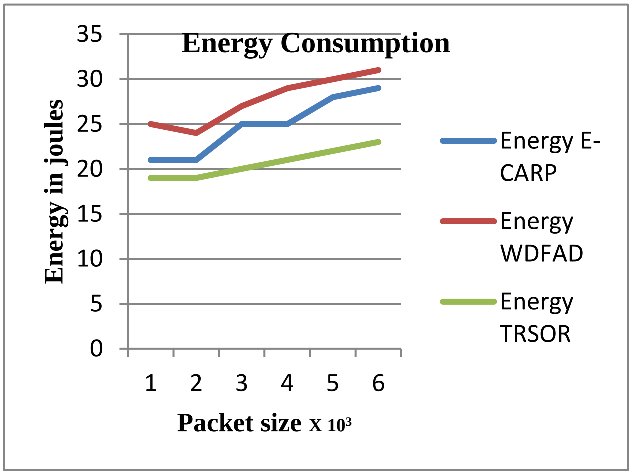

Figure 2: Energy consumption Comparison Chart

Figure 2 illustrates the time synchronization with energy consumption. In the TRSOR method, energy consumption is very less. The E-CARP and WDFAD methods are high energy consumption of active nodes. The X-axis represents the time in seconds, and the Y-axis represents the energy level.

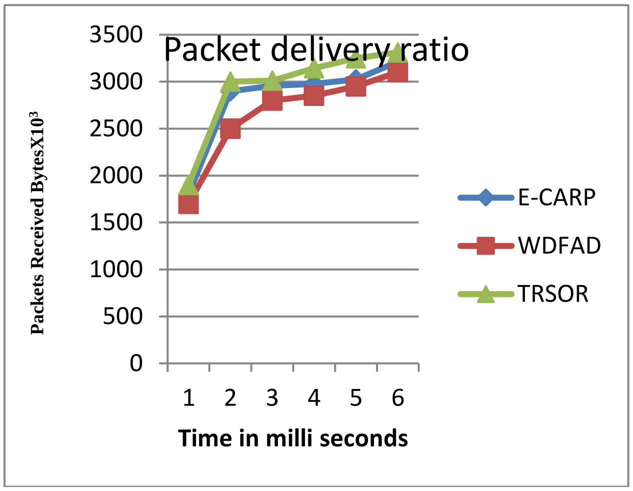

Figure 3: Packet Delivery ratio

Figure 3 illustrates the data flow level by packet transmission: the E-CARP and WDFAD methods are used as low data flow levels. The TRSOR method has a high data flow level by comparing the existing methods. The X-axis represents the data flow in seconds, and the Y-axis represents the packets.

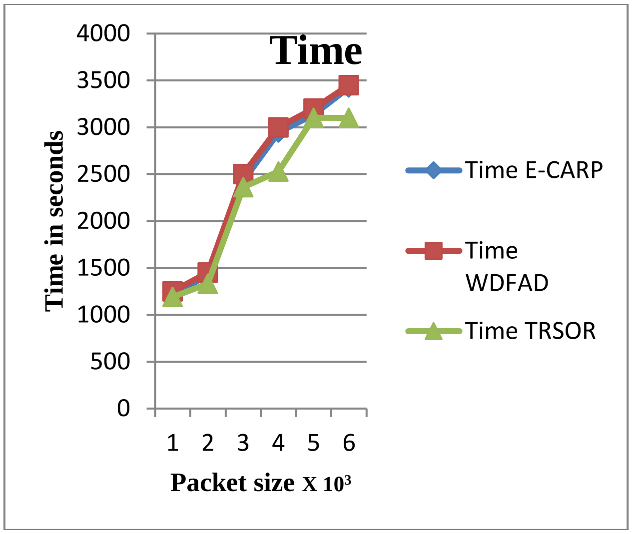

Figure 4: Transmission Time

Figure 4 illustrates the data transmission delay. The E-CARP and WDFAD methods are used for a high transmission delay. The TRSOR method has less time in transmission. This graph depicts the time in milliseconds along the Y axis and the sink node along the X axis.

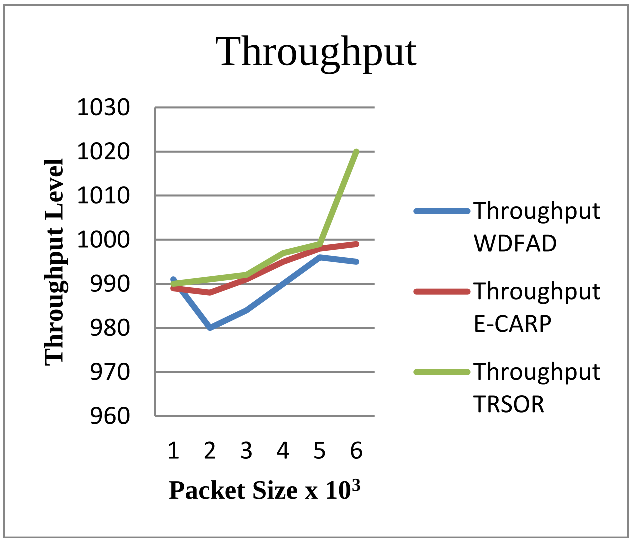

Figure 6: Throughput Comparison Chart

Figure 6 illustrates the Routing with throughput. The accuracy of TRSOR is increasing the message communication. It shows the throughput comparison; When compared to the E-CARP and WDFAD techniques, the TRSOR has higher throughput. The X-axis shows the passage of time, while the Y-axis shows the throughput levels.

CONCLUSION

By relaying packets via intermediate nodes, this study shows how trustworthy-based opportunistic Routing in UWSNs may mitigate the problem of erratic acoustic transmission. TRSOR, an opportunistic routing technique, was suggested to reduce packet loss by effectively skipping vacant zones and optimizing transmission reliability in places with significant ambient noise and channel desertion. Periodic beaconing provides TRSOR with useful local knowledge, which is used to construct an adjacency graph, group nodes into contiguous clusters when possible, and utilize a cost-effective heuristic to find the best route between nodes in each cluster. While other literature-described protocols guide all packets toward the surface, TRSOR is flexible enough to send data in any direction while avoiding unnecessary hops. Our simulations show that TRSOR can significantly reduce packet loss, energy consumption, and end-to-end latency in sparse and congested network situations.

References

[1] Arifeen, M. M., Islam, A. A., Rahman, M. M., Taher, K. A., Islam, M. M., & Kaiser, M. S. (2019). ANFIS-based Trust Management Model to Enhance Location Privacy in Underwater Wireless Sensor Networks. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). doi:10.1109/ecace.2019.8679165

[2] Basagni, S., Petrioli, C., Petroccia, R., & Spaccini, D. (2012). Channel-aware Routing for underwater wireless networks. 2012 Oceans - Yeosu. doi:10.1109/oceans-yeosu.2012.6263538

[3] Coutinho, R. W. L., Boukerche, A., Vieira, L. F. M., & Loureiro, A. A. F. (2016). Geographic and Opportunistic Routing for Underwater Sensor Networks. IEEE Transactions on Computers, 65(2), 548-561. doi:10.1109/tc.2015.2423677

[4] Coutinho, R. W. L., Boukerche, A., Vieira, L. F. M., & Loureiro, A. A. F. (2014). GEDAR: Geographic and opportunistic routing protocol with Depth Adjustment for mobile underwater sensor networks. 2014 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2014.6883327

[5] Darehshoorzadeh, A., & Boukerche, A. (2015). Underwater sensor networks: a new challenge for opportunistic routing protocols. IEEE Communications Magazine, 53(11), 98-107. doi:10.1109/mcom.2015.7321977

[6] Draz, U., Ali, T., Yasin, S., Fareed, A., & Shahbaz, M. (2019). Watchman-based Data Packet Forwarding Algorithm for Underwater Wireless Sensor and Actor Networks. 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). doi:10.1109/icecce47252.2019.8946

[7] Emokpae, L., & Younis, M. (2012). Signal reflection-enabled geographical routing for underwater sensor networks. 2012 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2012.6363766

[8] Ghoreyshi, S. M., Shahrabi, A., & Boutaleb, T. (2016). An Opportunistic Void Avoidance Routing Protocol for Underwater Sensor Networks. 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). doi:10.1109/aina.2016.96

[9] Hsu, C.-C., Liu, H.-H., Garcia Gomez, J. L., & Chou, C.-F. (2015). Delay-Sensitive Opportunistic Routing for Underwater Sensor Networks. IEEE Sensors Journal, 15(11), 6584–6591. doi:10.1109/jsen.2015.2461652

[10] Ismail, M., Islam, M., Ahmad, I., Khan, F. A., Qazi, A. B., Khan, Z. H., … Al-Rakhami, M. (2020). Reliable Path Selection and Opportunistic Routing Protocol for Underwater Wireless Sensor Networks. IEEE Access, 1–1. doi:10.1109/access.2020.2992759

[11] Jiang, J., Han, G., Zhu, C., Chan, S., & Rodrigues, J. J. P. C. (2017). A Trust Cloud Model for Underwater Wireless Sensor Networks. IEEE Communications Magazine, 55(3), 110–116. doi:10.1109/mcom.2017.1600502cm

[12] Karim, S., Shaikh, F. K., Chowdhry, B. S., & Otero, P. (2020). Geographic and Cooperative Opportunistic Routing Protocol for Underwater Sensor Networks. 2020 Global Conference on Wireless and Optical Technologies (GCWOT). doi:10.1109/gcwot49901.2020.939176

[13] Khan, A., Javaid, N., Mahmood, H., Sangeen, Khan, Z. A., & Qasim, U. (2016). EEIRA: An Energy Efficient Interference and Route Aware Protocol for Underwater WSNs. 2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS). doi:10.1109/cisis.2016.129

[14] Krishnaswamy, V., & Manvi, S. S. (2021). Trusted node selection in clusters for underwater wireless acoustic sensor networks using fuzzy logic. Physical Communication, 47, 101388. doi:10.1016/j.phycom.2021.101388

[15] Mohamad, M. M., & Kheirabadi, M. T. (2016). Energy efficient opportunistic routing algorithm for underwater sensor network: A review. 2016 2nd International Conference on Science in Information Technology (ICSITech). doi:10.1109/icsitech.2016.7852605

[16] Sahana, S., Singh, K., Das, S., & Kumar, R. (2016). Energy efficient shortest path routing protocol in underwater sensor networks. 2016 International Conference on Computing, Communication and Automation (ICCCA). doi:10.1109/ccaa.2016.7813780

[17] Tonghong Li. (2008). Multi-sink opportunistic routing protocol for underwater mesh network. 2008 International Conference on Communications, Circuits and Systems. doi:10.1109/icccas.2008.4657802

[18] S. Wang, T. L. N. Nguyen and Y. Shin, "Data Collection Strategy for Magnetic Induction Based Monitoring in Underwater Sensor Networks," in IEEE Access, vol. 6, pp. 43644-43653, 2018, doi: 10.1109/ACCESS.2018.2861946.

[19] Wadud, Z., Ismail, M., Qazi, A. B., Khan, F. A., Derhab, A., Ahmad, I., & Ahmad, A. M. (2019). An Energy Balanced Efficient and Reliable Routing Protocol for Underwater Wireless Sensor Networks. IEEE Access, 7, 175980–175999. doi:10.1109/access.2019.2955208

[20] Zhou, Z., Yao, B., Xing, R., Shu, L., & Bu, S. (2016). E-CARP: An Energy Efficient Routing Protocol for UWSNs in the Internet of Underwater Things. IEEE Sensors Journal, 16(11), 4072–4082. doi:10.1109/jsen.2015.2437904