Underwater Wireless Sensor Network Route Optimization using BIHH Technique

Turki Ali Alghamdi
Department of Computer Science
College of Computer and Information Systems
Umm Al-Qura University, Makkah. Saudi Arabia

Abstract—**Underwater wireless sensor network (UWSN) is established in water bodies such as oceans, seas and rivers to observe the activity of military, to perform rescue operations and to do mining activity of resources. The sensor nodes communicate through acoustic channels. These nodes have limited battery life (energy), narrow bandwidth and a channel is incurred with delays and noise posing security thrust. The art of work presented different routing protocols in this era to utilize energy and bandwidth efficiently with less delay and to provide the security against black hole attack. However, these methods do not show an appropriate enhancement in the security and to utilize the bandwidth efficiently due to mobile environment. As a result of which, the delay also increases. In this paper a secured and bandwidth utilization path is enhanced using Bellman Inora Hex Hamming technique (BIHH), which not only improves the performance of the routing but also saves the energy. The presented approach is validated with network simulator.**

Keywords—Sensor nodes; energy; routing; black hole; hamming code; hex code

I. Introduction

Underwater communication becomes necessary to the entire world to obtain necessary information about the underwater resources (e.g. minerals), to check the occurrence and frequencies of tsunamis and to monitor the warfare environment. These issues change the mindset of the research community to work in this era. The method is about transmitting and getting communication under the exploitation of sound transmission in underwater atmosphere and it is acknowledged as an acoustical or an audio communication. The Underwater sensor networks (UWSNs) comprise numerous sensors and vehicles to be organized in a particular area, to complete joint observation and to gather the data tasks [1]. Conventionally for observation of sea base, the ocean sensors are used to monitor the information at a fixed position and recuperate the equipment's at the end of assignment. The drawback of the conventional technique is that it lacks the cooperation in the announcement among dissimilar ends, the monitored data is of no use and in the case of any collapse, and the monitored information will be damaged.

The main key issue of UWSNs is node mobility (i.e. mobility of node is almost 2-3m/sec. due to water currents [2]) and energy of the nodes. Several techniques have been proposed to address these issues. However, few gaps still exist (i.e. usage of bandwidth, security of the network and delay in the network). Therefore, an efficient routing protocol is needed to UWSNs which can improve the energy, bandwidth, and security and reduces the end to end delay.

In this paper, an efficient path estimation technique is being presented using Bellman Inora Hex Hamming (BIHH) technique. This protocol also provides security to UWSNs against well-known attack called black hole attack which is very common type of attack to mobile sensor network.

The remaining part of the paper is discussed as Section 2 represents related work, Section 3 represents the proposed technique, and Sections 4 and 5 represents the simulation results and conclusion of the paper, respectively.

II. Related Work

Cinar and M. Bulent Orencik [3] proved that sensor networks in underwater have wide range of applications such as pollution check in sea and rivers, monitoring wind pressure, aquatic surveillance and can also be used to monitor the warfare environment. Underwater Sensor Network (UWSN) with the acoustic channel is the only technique that can be used to measure various network parameters in the sea [4, 5], as it is considered that the velocity of sound is constant in underwater. But the velocity is changed by temperature difference, salinity and depth of the water. As a result of which sound in underwater environment varies [6]. Due to characteristics change in underwater environment, it becomes challenging to utilize the acoustic channel [7] (e.g. multipath environment effects the phase and fading fluctuations, Doppler Effect is present at both source and destination nodes). In [8-10] comparison of the weaknesses and strengths of MAC layer protocols for both single and multipath environment in underwater sensor networks is presented. The three-dimensional network arrangements and the ground level of the ocean are observed by anchoring sensor nodes [11-13].

In [14, 15] the authors presented routing protocols for UWSNs in which network lifetime has been improved. To achieve this goal the authors used autonomous vehicle to collect the data from gateways and used shortest path to transfer the data from sensor nodes to gateways, by minimizing the associated nodes in the network. However, minimization of nodes in the path increases delay and packet delivery ratio is reduced. Jing Li et al. [16] presented an energy efficient protocol for UWSNs, in which packet delivery ratio is improved by managing the energy and power allocation. However, the given algorithm is more complex and enhances the delay which in turn reduces the overall output and may not be suitable for real time applications. Faheem. M et al. [9] presented a quality of service (QoS) routing protocol for UWSNs based on clustering technique. But due to autonomous structure it is difficult to maintain cluster head for long period of time and therefore reduces the routing performance.

Zhiping Wan et al. [17] proposed an energy efficient multilevel routing algorithm for UWSNs. In this algorithm a hierarchical structure based on residual energy was designed to calculate the competition radius size. However, checking the residual energy continuously decreases the packet delivery ration. Meiju Li et al. [18] presented a shortest path routing technique for underground water acoustic networks based on vertical angle. In this algorithm prioritization concept is used to check the vertical angle at every anchoring sensor node till it reaches to destination which increases the complexity and reduces throughput. M. Awais et al. [19] presented an energy efficient algorithm using void-hole alleviation technique. In this method the forwarding node determines the next hop. However, two same hops with different link weights may have different delays (i.e. more is the link weight more will be the delay) so cannot be treated as optimum route from source to destination. Adil et al. [20] proposed an energy efficient method for UWSNs using EH-ARCUN technique. This method entirely depends on cooperation of sensor nodes within the network, so may not be suitable for heterogeneous networks. In [21, 22] two different energy efficient routing protocols have been proposed using IoT, however both the two techniques maximize the delay as number of IoT sensors are employed in the existing network. So, may not be the optimum for real time applications. UWSN has several challenges i.e. bandwidth, error rate and failure of the route. This includes mobility of 2-3 m/sec. at water current [23].

From the above theories and models, it has been observed that path has been optimized either by energy (i.e. using clustering technique, minimization of nodes etc. and inserting number of sensor nodes in the network) or choosing the shortest path between end nodes. However, both the two may not be the optimum as the delay parameter is increased with these approaches, which in turn maximizes the consumption of energy and reduces the overall throughput and packet delivery ratio, so may not be optimum for real time applications. Also, along with the above mentioned issues this security against malicious node attack must be enhanced, because these attacks have been addressed in the UWSN using key distribution which may not always true and optimum due to an autonomous structure. For route optimization, a model must be proposed that can overcome these issues.

In this paper, a secured and efficient path optimization technique is being presented which improves the throughput, utilizes the bandwidth efficiently and enhances the energy. Also, the paths from source to destination are being ranked based on link cost and its energy. In addition, security is also been provided to the network, unlike the conventional techniques which considers only energy or only the shortest distance of the links between the nodes.

III. Proposed Approach

Under water wireless sensor network have numerous challenges, such as consumption of energy, optimization of path from source to destination, utilization of bandwidth and security. In this paper, the main focus is given towards the path estimation and security against black hole attack, which is common attack in this network. To achieve this goal, the paper has three folds.

- Estimation of paths from source to destination and rank them.
- Establishment of alternate route in case of failure based on the rank of the path (from source to destination).
- Security against black hole attack.

A. *Estimation of Path*

To estimate the path from source to destination, Bellman Ford technique is used to obtain the least cost path between end nodes. Initially the approach estimates calculation of ‘m’ nodes that involves the cost of each of its neighboring node links from a definite source node ‘S_N’ ($d_i^{(H)}$) where ‘H’ is the hop count. It is assumed that each node has a link cost and paths for other nodes, which are available in the network. Also, the information which is available with the node can be exchanged directly to its neighboring nodes in regular time intervals. Based on this information it updates the link cost and the available paths. The notations used to describe this technique can be represented as

M = No of nodes

S_N = Source node

N = Number of nodes which are incorporated within this approach

lc_{ij} = Cost of the link from ith node to jth node

However, if the node are not connected directly then ‘$lc_{ii} = 0$’ and ‘ $lc_{ij} = \infty$’. Whereas if ‘$lc_{ij} \geq 0$’, then nodes are connected directly.

$P_{lc(m)}$ = least cost path from ‘S to m’, under the limit that the links should not more than ‘p’.

p = max. links in the path

Algorithm

The following are the steps of algorithm to find the shortest path, however step 2 repeats the link cost change.

```
1.  Initialize
    $p^0_{lc(m)} = \infty, \forall\, m \neq S_N$
    $p^{(P)}_{lc(S)} = 0, \forall\, P$
2.  For every consecutive ‘P ≥ 0
        $p^{(P+1)}_{lc(m)} = {}^{min}{}_{j}[p^{(P)}_{lc(j)} + p_{lc(jm)}]$
```

The route from source node ‘S_N’ to ith node stops with the cost of link from node ‘j’ to node ‘i’.

For step 2 iteration with ‘H = Q’, and for every sink node ‘m’ this technique analyzes and compares the routes from ‘S to m’ of length ‘Q + 1’ with the obtained route in pervious iteration. If the previous route is shorter, it retains this path as the path with low cost. Else the new obtained path i.e. ‘Q+1’ is employed from source to destination. Thus, this route is of distance ‘Q’ from ‘S’ to other node say ‘j’ with addition of a hop directed from ‘j’ to node ‘m’. Also, it will maintain the route information with the source node till route from source to destination is finalized.

Example:

Fig. 1 represents an underwater wireless sensor network deployed in a certain geographical area, in which a source node ‘S_N’ and destination node ‘D_N’ is deployed at ground. However intermediate nodes i.e. A, B, C and E are deployed in under water.

Let the source node wants to communicate with the destination node through these underwater intermediate sensor nodes. Initially, the source node interacts with its neighboring nodes which are one hop away from it and makes that path permanent whose link cost is low in comparison with the other neighboring nodes at hop 1. However, the source has the node and link information of all its neighboring nodes at hop 1. This process of finalizing the path at various hops will continue till completion of communication between end nodes.

Operation at hop 1: As per the model description there are two neighboring nodes (i.e. A and B) of source node ‘S_N’, Table I represent the path and link cost at hop 1. The other nodes at hop 1 are not accessible, so can be represented by ‘∞’.

The link cost of node ‘B’ is less as compared with node ‘A’. Hence node ‘B’ will be treated as permanent node for path calculation. However, the path and link cost information will be available with the source node till finalization of the path is done between end nodes.

Operation at hop 2: Table II represent the path and link cost at hop 2. In this stage there are three neighboring nodes (i.e. B, E and C), so the possible paths at this hop will be three (see Table II).

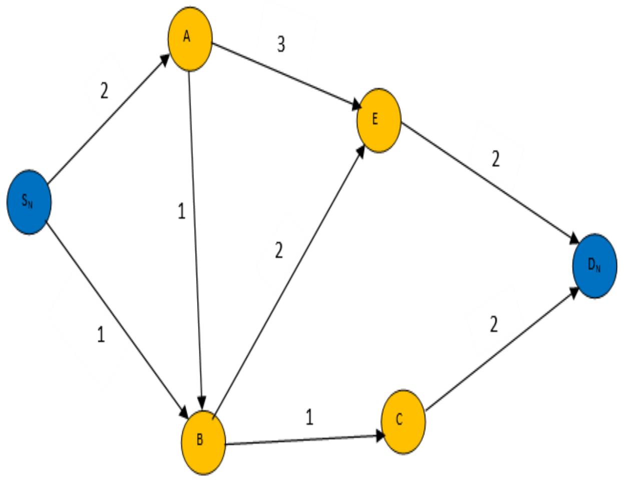

Fig. 1. Wireless Sensor Network.

TABLE I. PATH AND LINK COST AT HOP 1

S. No	Path	Link Cost
1	S_N- A	2
2	S_N- B	1

TABLE II. PATH AND LINK COST AT HOP 2

S. No		Path	Link Cost
1		S_N- A- B	3
2		S_N- A - E	5
3		S_N- B - C	2
4		S_N- B - E	3

Out of these three paths the proposed technique will select S_N-B-C path and make the node ‘C’ as permanent node, as the link cost of this path is having less value as compared to the other two. Also, the other routes information will be available with the source node. Again, the destination node is not accessible hence can be represented by ‘∞’.

Similarly, the operation at hop 3 and hop 4 can be represented in Tables III and IV, respectively.

At this stage (i.e. at hop 3 as per the Table III) the given technique will choose ‘S_N- B – C – D_N’ path, as destination is achieved directly. Though the destination node is reached in hop 3 the other hops in the path estimation is evaluated so as to give the rank to all the possible paths from source to destination.

Again, the pervious path will be chosen as the optimum path because the link cost is less between end nodes. However, in case of failure of path due to unavailability of bandwidth or occurrence of congestion at the node, it will choose the route which will have the next least link cost. If the two paths have same link cost, it will choose the route which has less involvement of nodes as it will have less nodal delay. So due to less involvement of nodes and choose of least cast path between end nodes, the consumed energy is reduced. Also, in case of failure of the route the next optimized path information is available with the preceding node that reduces further nodal time (i.e. propagation, queuing, transmission and processing time). Which intern saves energy of the network and enhances the lifetime of the node in terms of energy consumption. The order (prioritization) of the paths from source to destination is represented in Table V.

The estimation of congestion occurrence and bandwidth unavailability is discussed in next section and accordingly the path from source to destination is finalized.

TABLE III. PATH AND LINK COST AT HOP 3

S. No	Path	Link Cost
1	S_N- A- B - E	5
2	S_N- A – E – D_N	7
3	S_N- A- B - C	4
4	S_N- B – C – D_N	4
5	S_N- B – E –D_N	5

TABLE IV. PATH AND LINK COST AT HOP 4

S. No	Path	Link Cost
1	S_N- A- B – E – D_N	7
2	S_N- A – B - C – D_N	6

TABLE V. PRIORITIZATION OF PATHS

S. No	Priority	Link Cost
1	S_N- B – C – D_N	4
2	S_N- B – E –D_N	5
3	S_N- A – B - C – D_N	6
4	S_N- A – E – D_N	7
5	S_N- A- B – E – D_N	7

B. Establishment of Alternate Route in Case of Failure

To get an alternate route Dharmaraju et al. [24] proposed a framework to guarantee the QoS (quality of service) routing. This framework makes use of INSIGNIA and TORA [25] to obtain multiple routes between end users. To get the QoS routing the work is subdivided into two types which are:

- Feedback based on coarse method
- Feedback based on class method

1) Coarse method: This method fails to provide the QoS, if a node has insufficient bandwidth available to transfer the information between end nodes or due to occurrence of congestion at a node. In this case a given node sends admission control failure (ACF) information to the upstream node. This node (upstream node) then selects the next optimum route to guarantee the QoS. The operation of this method is explained by considering the following example.

Example:

Fig. 2 represents the application of coarse feedback technique in wireless sensor network. As per the given method let the route created by directed acyclic graph (DAG) available be the shortest path i.e. S_N – B- C- D_N.

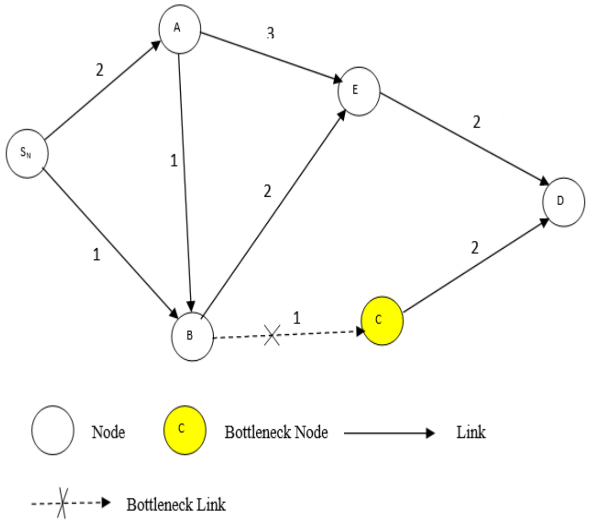

Fig. 2. Coarse Feedback.

Assume node ‘C’ may not be able to admit the data flow due to unavailability of resources. So, it sends an ACF (Authentication control function) from node ‘C’ to node ‘B’, then node ‘B’ checks the feasible path among its neighbors. Here node ‘E’ is the only available node that can forward the data flow towards the destination node. Thus, the feasible path available which can guarantee the QoS is ‘S_N– B – E – D_N’.

Let node ‘E’ fails to receive the data flow, it will also send an ACF information to node ‘B’ and it will send ACF message to source node ‘S_N’ and source node makes use of another neighboring node and try to finalize the route. If source node will not get any path that can guarantee the QoS, it will simply reject the flow.

2) Class method: In this type the period between $(Min)_{B.W}$ and $(Max)_{B.W}$ is divided into ‘X’ classes, where $(Min)_{B.W}$ and $(Max)_{B.W}$ are the bandwidths required to generate the flow. Let the source node is ready to transmit the information towards sink node and the transmitted data flow is of class ‘r (r< X)’. Consider a wireless sensor network as shown in Fig. 3 and the path created by DAG is ‘S_N – B- C- D_N’.

The node ‘B’ accepts the data flow with ‘r’ class effectively and node ‘C’ accepts the data flow whose bandwidth lies in class ‘p’ (p < r) only. At this stage node ‘C’ transmits Admission Report information (AR (p)) to upstream node i.e. ‘B’ to indicate that it has the ability to consider only ‘p’ bandwidth that can be accepted by it. To solve this issue node ‘B’ divides the data flow at a ratio of ‘p to r – p’ and transmits the flow to node ‘C’ and node ‘E’ in the given ratio. The ‘r’ class node is divided into two flows, if ‘E’ node will give the class ‘r – p’ as requested by node ‘B’. The two flows, one with the bandwidth of ‘p’ class having path ‘S_N – B- C- D’. However, if node ‘E’ accepts only class ‘h (h < r- p)’, it transmits an AR (h) information to node ‘B’.

If the other neighbors of node ‘B’ are not able to provide the ‘r’ class facilities, it sends AR (p+h) to source node as it has the ability to provide class services of (p + r). Then the source node finds another anchoring node which can provide the facility to accept the flow of class (r – (p +h)), however if source node will not find any such node, it simply rejects the flow.

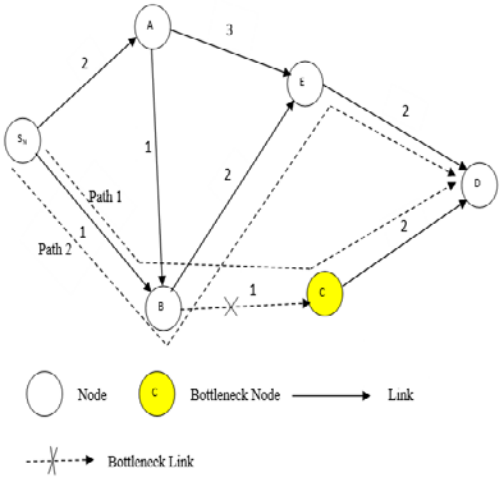

Fig. 3. Class Feedback.

C. Security Against Black Attacks

Due to autonomous structure sensor, the network possesses a well-known security threat called Black Hole Attack. Several models have already been proposed e.g. [26, 27] to detect this attack using distribution of keys. However, due to autonomous structure key distribution is difficult as nodes can move in and out of the network at any time instant. Assignment of keys is favorable in the network with static nodes and may not be effective for the network with mobile nodes. In this paper, a black hole attack is detected using hamming and hex coding technique and is excluded from any route (from source to destination) at any hop in the network. As the coding is kept simple it will not increase the complexity and reduce delay. Let Fig. 4 represents the wireless sensor environment with a black hole in the network.

In the presented approach the code at source is binary hex value of decimal ‘1’ (i.e. 1= 0001). Therefore, the hamming bit positions will be at ‘2^{n}’ where ‘n = 0,1 and 2 in this case’, as we are considering only 4-bit code at source.

Hamming bit positions (HP) P1 P2 D P4

Source code (SC) 0 0 0 1

However, if one can increase the code length, hamming bits will also increase. The security code at various hops can be generated using compliment to hamming bits with respect to hop count. So, the compliment bits at various hops can be represented as

$$B_{ch} = \bar{P}_{(2)^n} \quad (1)$$

Where ch = hop number and ‘n =0, 1and 2’ for hop 1, 2 and 3 respectively. So, the security code-word at hop ‘1’ will be “1001”. Similarly, the security codeword bits at hop 2 and 3 are generated by complimenting remaining parity bits (one at each hop) as given in eq. (1). Table VI shows the security codes of hops 1, 2 and 3. After ‘3rd’ hop the security code repeats.

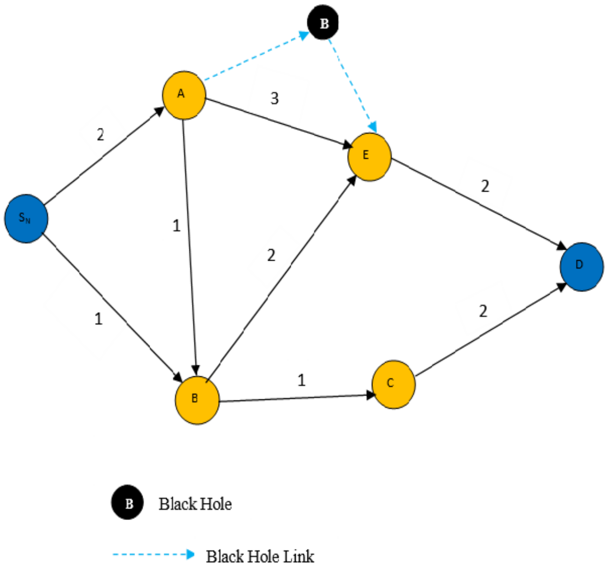

Fig. 4. Wireless Sensor Network with Black Hole Attack.

TABLE VI. SECURITY CODE AT VARIOUS HOPS

Source code		0 0 0 1			
Hamming Parity bits		P_1 P_2 D P_4			
S. No	Hop count	Security code			
1	1	1	0	0	1
2	2	1	1	0	1
3	3	1	1	0	0

1) *Node matching process:* Let the source node is ready to transmit the information to destination node through intermediate nodes. So at hop ‘1’ node ‘A’ and node ‘B’ are the only nodes which can take part in the network, as both the two nodes are active and knows the security operation at hop ‘1’, therefore can be able to generate the security code at this hop and match with the source node and source node can transmit the information to both the two nodes.

Now at hop ‘2’ nodes ‘C, B and E can take part in the network. Out of the three nodes, node ‘B’ cannot judge the security code at this hop because it doesn’t know the security operation at this particular hop and cannot match with the code word of the upstream node. Therefore, can be easily detected and will not allow taking part with the network nodes. Similarly, at other hops this process of node matching and removal of black hole will continue till the information reaches the destination.

IV. SIMULATION RESULTS

The stimulation tool which is used to validate the proposed approach is Network Simulator. The network used is multi-hop, protocol used is MAC and the number of nodes considered in the network is 250 with node mobility above 0.2 m/s. The simulation parameters are briefly discussed in Table VII. The presented approach is compared with the Faheem, Zhiping and Meiju approaches as they are the recent methods proposed in this field.

Fig. 5 represents the variation of energy with respect to the nodes. From the figure, it is observed that the overall energy consumed by the presented approach is less when compared with the other techniques as only the QoS route is considered which minimizes the energy consumed, hence optimizes the energy of the nodes that can take part in the route.

Fig. 6 represents the variation of loss rate with respect to the no of packets sent. It is clear from the figure that the presented approach has less packet loss rate. As it utilizes the bandwidth efficiently to avoid the path in which congestion may occur. Because it selects the next alternate optimum path between end nodes to avoid packet loss.

The variation of overhead with respect to the number of hops is represented in Fig. 7 with least packet overhead of the presented approach in comparison with the conventional techniques as the congestion is avoided which minimizes the overhead.

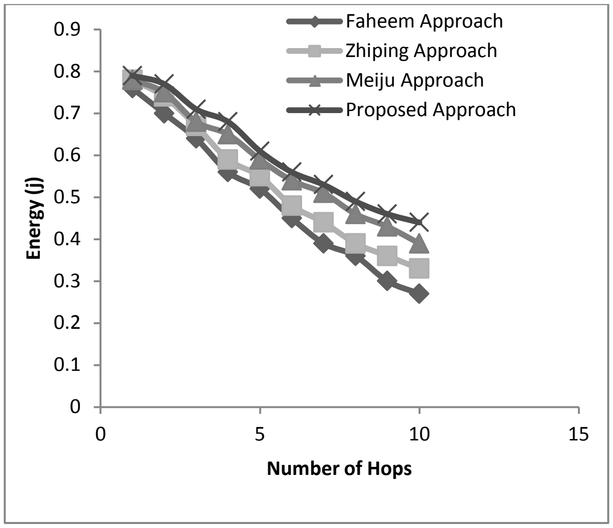

Fig. 5. Energy Saved Versus Number of HOPS.

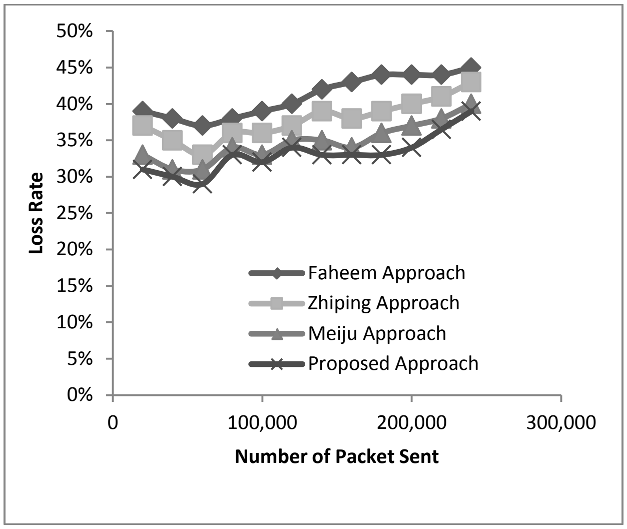

Fig. 6. Loss Rate Versus Packet Sent.

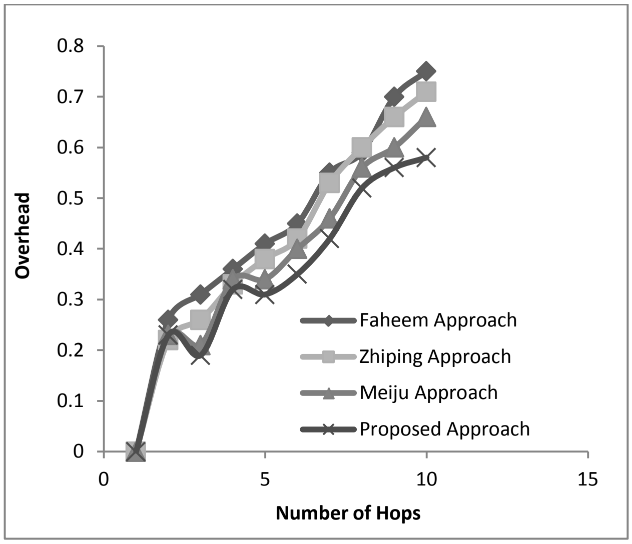

Fig. 7. Overhead Versus Number of HOPS.

TABLE VII. SIMULATION PARAMETERS

S.No	Parameters	Value
1	Underwater Monitoring Area	400m x 400m x400m
2	Maximum speed of node mobility	3m/s
3	Minimum speed of node mobility	0.2m/s
4	MAC	8.11
5	Number of black holes	23
6	Node communication radius (mts)	230
7	Packet size (bits)	512
8	Packet header (bits)	100
9	Initial energy of sensor node (j)	10

V. CONCLUSION

The presented approach is simple and effective for the research community to enhance their work for underground water sensor network. The presented approach considers multiple QoS parameters for choosing a route from source to destination. This approach also ranks the paths in case of any failure occurred due to unavailability of bandwidth or congestion at any node. Security against black hole attack is also an enhancement to the proposed approach.

REFERENCES

[1] N. Ismail, L. A. Hussein, and S. H. S. Ariffin, “Analyzing the performance of acoustic channel in underwater wireless sensor network (UWSN)”, in Proceedings of the Asia Modeling Symposium 2010: 4thInternational Conference on Mathematical Modelling and Computer Simulation, AMS2010, pp. 550–555, Malaysia, May 2010.

[2] K. Awan, P. Shah, K. Iqbal, S. Gillani, W. Ahmad, and Y. Nam, “Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges”, Wireless Communications and Mobile Computing Volume 2019, Article ID 6470359, pp 1-20 https://doi.org/10.1155/2019 /6470359

[3] T. Cinar and M. Orencik, “An underwater acoustic channel model using ray tracing in ns-2”, in Proceedings of the 2009 2nd IFIP Wireless Days (WD 2009), pp. 1–6, Paris, December 2009.

[4] M. Ayaz and A. Abdullah, “Underwater wireless sensor networks: Routing issues and future challenges”, in Proceedings of 7thInternational Conference on Advances in Mobile Computing and Multimedia, MoMM2009, pp. 370–375, Malaysia, December 2009.

[5] L. Liu, S. Zhou, and J. H. Cui, “Prospects and problems of wireless communication for underwater sensor networks”, Wireless Communications and Mobile Computing, vol. 8, no. 8, pp.977–994, 2008.

[6] G. Zaibi, N. Nasri, A. Kacouri, and M. Samet, “Survey of temperature variation effect on underwater acoustic wireless transmission”, ICGST-CNIR Journal, vol.9, pp 1-6, 2009.

[7] X.-P.Gu,Y.Yang and R.L.Hu, “Analyzing the performance of channel in Underwater Wireless Sensor Networks (UWSN)”, in Proceedings of the 2011 International Conference on Advanced in Control Engineering and Information Science, CEIS2011, pp. 95– 99, China, August 2011.

[8] N. Li, J. Martínez, J. Chaus, and M. Eckert, “A survey on under water acoustic sensor network routing protocols”, Sensors, vol.16, no.3,414,2016.

[9] M. Faheem, G. Tuna, and V. Gungor, “QERP: Quality of Service (QoS) Aware Evolutionary Routing Protocol for Underwater Wireless Sensor

Networks”, IEEE Systems Journal, vol 12, issue 3, pp 2066-2073, sept. 2018.

[10] C. Zidi, F. Bouabdallah, and R. Boutaba, “Routing design avoiding energy holes in underwater acoustic sensor networks”, Wireless Communications and Mobile Computing, vol. 16, no.14, pp.2035–2051, 2016.

[11] I. Akyildiz, D. Pompili, and T. Melodia, “Underwater acoustic sensor networks: research challenges”, AdHoc Networks, vol.3, no.3, pp. 257–279, 2005.

[12] I. Akyildiz, D.Pompili, and T. Melodia, “Challenges for efficient communication in underwater acoustic sensor networks”, SIGBED Review, vol.1, no.2, pp.3–8, 2004.

[13] C. Peach and A. Yarali, “An Overview of Underwater Sensor Networks”, in Proceedings of the routing techniques regarding network layer, pp.31–36,2013.

[14] N. Javaid., N. Ilyas., A. Ahmad, et al. “An efficient data gathering routing protocol for underwater wireless sensor networks”, Sensors. Vol 15(11), pp 29149–29181 (2015).

[15] N. Ilyas, T. Alghamdi, M. Farooq, B. Mehboob, A. Sadiq, U. Qasim, Z. Khan and N. Javaid, "AEDG: AUV-aided Efficient Data Gathering Routing Protocol for Underwater Wireless Sensor Networks,", Procedia Computer Science, vol. 52, no. 1, pp. 568-575, Jun 2015.

[16] Jing, L., He, C., Huang, J., et al.: Energy management and power allocation for underwater acoustic sensor network. IEEE Sens. J. vol 17(19), pp 6451–6462 (2017).

[17] Zhiping Wan. Shao jiang Liu. Weichuan Ni. Zhiming Xu’ “An energy-efficient multi-level adaptive clustering routing algorithm for underwater wireless sensor networks,” clustering computing, vol 22, pp 14651-14660, March 2018.

[18] Meiju Li, Xiujuan Du, Xin Liu, and Chong Li, “Shortest Path Routing Protocol Based on the Vertical Angle for Underwater Acoustic Networks,” Journal of Sensors Volume 2019, Article ID 9145675, pp 1-14, https://doi.org/10.1155/2019/9145675.

[19] M. Awais, I. Ali, T. Alghamdi, M. Ramzan, M. Tahir,M. Akbar, N.Javaid, "Towards Void Hole Alleviation: Enhanced GEographic and Opportunistic Routing Protocols in Harsh Underwater WSNs", in IEEE Access, vol. 8, pp. 96592-96605, 2020, doi: 10.1109/ACCESS. 2020.2996367.

[20] Adil Khan,Mukhtaj Khan, Sheeraz Ahmed, MohdAmiruddin Abd Rahman, Mushtaq Khan, “Energy harvesting based routing protocol for underwater sensor networks,” PLOS ONE | vol 14(7) https://doi.org/10.1371/journal.pone.0219459 July 17, 2019.

[21] Pan Feng, Danyang Qin, Ping Ji, Min Zhao, Ruolin Guo and Teklu Merhawit Berhane, “Improved energy-balanced algorithm for underwater wireless sensor network based on depth threshold and energy level partition” EURASIP Journal on Wireless Communications and Networking (2019) 2019: vol 228, pp 1-15 https://doi.org/10.1186/s13638-019-1533-y.

[22] S. Butt, K. Bakar, N. Javaid et al., “Exploiting layered multipath routing protocols to avoid void hole regions for reliable data delivery and efficient energy management for IoT enabled underwater WSNs,” Sensors, vol.19, no.3, article no.510,2019.

[23] S. Ashraf, A. Raza, Z. Aslam, H. Naeem and T. Ahmed, “Underwater Resurrection Routing Synergy using Astucious Energy Pods”, Journal of Robotics and Control, vol 1, pp 173-184 (2020)

[24] D. Dharmaraju, A. R. Chowdhury, P. Hovareshti, and J.S Baras, “INORA. A unified signaling and routing mechanism for QoS support in Mobile Adhoc Networks,” proceedings of ICPPW 2002. pp 86-93.

[25] C.R. Lin and M. Gerla, “Real time support in multihop wireless networks,” ACM/ Baltzer Wireless Networks Journal, vol 5, no 2, pp 125-135,1999.

[26] W. A. Xiong and Y. H. Gong, “Secure and Highly Efficient Three Level Key Management Scheme for MANET’, Proc. of WSEAS Transactions on Computers, vol. 10, pp. 6-15, 2011.

[27] M. Celestin, S. Vigila, and K. Muneeswaran, “Implementation of text-based cryptosystem using Elliptic Curve Cryptography”, Prof. of 1st Int. Conf. on Advanced Computing, vol. 9, pp. 82-85, 2009.