Underwater Wireless Sensor Networks (UWSN), Architecture, Routing Protocols, Simulation and Modeling Tools, Localization, Security Issues and Some Novel Trends

S. EL-Rabaie[1], D. Nabil, R. Mahmoud and Mohammed A. Alsharqawy[2]
[1]Faculty of Electronic Engineering, Dept. of Communication Engineering, 32952 Menouf, EGYPT
[2]Egyptian Radio & Television Union (ERTU), Cairo, EGYPT
[1]srabie1@yahoo.com,[2]mnm_1946@hotmail.com

Abstract— Underwater wireless sensor networks (UWSNs) are becoming popular everyday due to their important role in different applications, such as offshore search and underwater monitoring. Underwater wireless sensor networks face unique conditions. Therefore, particular routing protocols are needed to route the packets from a source to a destination. Moreover, numerous UWSN's applications require deploying the security issue; which routing protocols don't take in consideration. A survey on UWSN architectural view and the routing protocols used for UWSNs are given in this paper. The routing protocols studied and compared with respect to packet delivery ratio, packet delay, energy consumption. Priority and drawbacks of each routing protocol are listed. In addition, a survey of the security issue for UWSNs is presented, and the security requirements in order to secure communication medium in this environment are listed

***Keywords*—**WSN, UWSN, Application, Design, Geographical routing, Security.

I.INTRODUCTION

The field of Wireless Sensor Networks (WSNs) has captured the imagination of the world with their potential to enhance human lives. WSN has wide applications in fields like agriculture monitoring, industrial monitoring, smart housing, automobile industry, and in military applications. Wireless sensor network (WSN) consists of a large number of small sensors capable of sensing, processing, and transmitting information to each other. These sensors communicate with other parts of networks using wireless interface. Figure 1 shows an example for WSN.

The design of WSNs depends on the environment, the applications objective, cost, hardware, and system constraints such as a limited energy, shortage of communication range and bandwidth, and limited processing and storage in each node. The environment determines the networks factors like size, topology andschemes. There are five types of WSNs: Terrestrial WSN, Underground WSN, Underwater WSN, Multi-media WSN, and Mobile WSN [1].

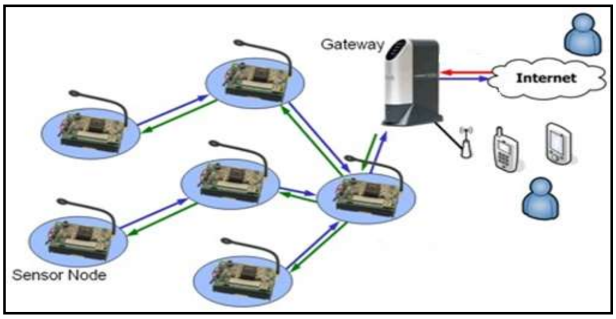


Fig. 1: Wireless Sensor Network.

– Terrestrial WSNs: Consist of a number of inexpensive wireless sensor nodes deployed in a given area.

– Underground WSNs: a number of nodes deployed underground to sense the surrounding conditions. Besides that, sink node is deployed to gather these sensed data to base station.

– Underwater WSNs: sensor nodes and vehicles form the networks used to monitor underwater conditions.

– Multi-media WSNs: Consist of a number sensor nodes equipped with cameras and microphones. Used to monitor and track events in the form of video, audio, and imaging.

– Mobile WSNs: Consist of nodes moves by itself which have the ability to reposition and organize itself in the network.

Large portion of ocean research conducted by placing sensors (that measure current speeds, temperature, salinity, pressure, chemicals, etc.) into the ocean and later physically retrieving them to download and analyze their collected data. This method does not provide real-time analysis of data, which is critical for event prediction. The real-time monitoring of underwater introduces the need of underwater wireless sensor networks. Underwater wireless sensor network communication has received increased attention motivated by many scientific, military, and commercial interests because it can enable a broad range of applications.

The major contribution of this paper is to give an introduction to underwater wireless sensor networks (UWSNs) its characteristic, challenges, applications, and architectures. A comparative study of some existing routing protocols, gives the advantages and limitations of one protocol over the others. Due to resource limitation, it is quite difficult to provide a strong security to UWSNs. This paper identifies the security requirements for UWSN, attacks against UWSNs, and particular solutions for these attacks. Furthermore, a security comparison between the existing routing protocols is given. This comparison clarifies the vulnerability of those routing protocols to various security attacks. Finally, the paper suggests new research directions as a future scope of study in UWSNs. In the rest of this paper, introduction to UWSNs its characteristic, challenges, applications, and architectures introduced in Section 2. Section 3 discusses some existing UWSNs routing protocols and give a comparison between them. In section 4, the security requirements, security attacks, and attacks defenses are presented. Section 5 elaborates the different model and simulation tools are used. Localization methods are outlined in Section 6. The proposed new directions of study are discussed in section 7. Finally, a brief conclusion is given in Section 8.

II.UNDERWATERWIRELESS SENSOR NETWORK (UWSN)

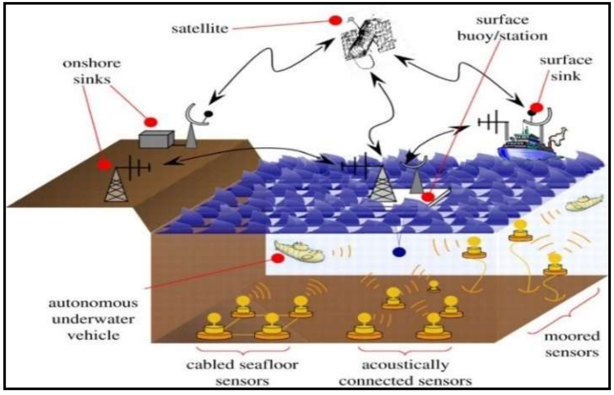


Fig. 2: Underwater Wireless Sensor Network.

From many decades, there has been a big interest in monitoring the underwater environment for scientific, commercial and military operations. Real time monitoring is very important for many applications, this calls the need of building Underwater Wireless Sensor Networks (UWSNs). UWSNs as seen in figure 2 consist of sensor nodes, surface stations and autonomous underwater vehicles (AUVs) networked to perform collaborative monitoring tasks.

1. UWSNs Challenges

The major challenges in the design of UWSNs are [2-4]:

– Underwater sensors are expensive in terms of equipment, deployment, and maintenance.

– Network Components: Underwater ordinary nodes, sinks, AUV, and onshore base station.

– The memory limited by the capacity of the on-board storage device.

– Battery power is limited and batteries cannot recharge, as solar energy cannot exploit.

– The available bandwidth is limited depending on the frequency. Acoustic systems operate below 30 kHz.

– Sensors are prone to failure because of fouling and corrosion and sensors size is large.

– Dynamic network topology, as nodes tend to be mobile, due to their self-motion capability or random motion of water currents.

– Routing: Due to high movement of nodes in water current.

– Range: Usually used in vast ocean areas.

– Propagation delay in underwater is higher than in channels of radio frequency terrestrial by five times.

– Connectivity loss and High bit error rates (shadow zones).

– The impaired channel due to multipath and fading.

– Reliability to guarantee the data is delivered to the surface sink.

– Time synchronization is difficult to achieve in the underwater because of spread delay and velocity of sound and so the localization.

– Variation in Sound Speed due to water conditions. Any change in one of these criteria affects sound speed. It may cause inaccuracy in position prediction.

2. UWSNs Communication System

Underwater communication system involves a transmission of information using any media, either acoustic waves, electromagnetic waves or optical waves [5].

- Electromagnetic Wave: The communication established at higher bandwidth and frequency. However, high absorption /attenuation cause limitation that alters the produced signal. Due to need to big size of antenna, cost and complexity of design increase.
- Optical Wave: Offer high data rate transmission. However, absorption and scattering effect influence the signal and the accuracy.
- Acoustic Wave: the low absorption of acoustic signal make it preferable in spite of its slow,

but the low absorption characteristic enables the signal pass long distance with small loss.

Table 1: A comparison between different modes of communication in UWSNs [5].

	Acoustic	Electromagnetic	Optical Waves
Speed (m/s)	1500	33,333,333	33,333,333
Bandwidth	1 KHz	1 MHz	10-150 MHz
Range	1 km	10 m	10-100 m
Power Loss	>0.1 dB/m/Hz	28 dB/1km/100MHz	depends on turbidity

3. *UWSNs***Architecture**

There are three different architectures for UWSNs [6]:

3.1 Static Two-Dimensional Underwater Sensor Networks

All the nodes anchored to the ocean floor. An uw-sink collects the data from the sensor nodes by the horizontal transceiver. Then, it relays the information to a surface station by the vertical transceiver.

The surface station has RF signal to communicate with the onshore and surface sinks, as shown in figure 3. The sensors communicated with the sink using direct links or multi-hop paths.

– In the direct link: each sensor directly sends data to the selected sink. This may not be the most energy efficient.

– In multi-hop path: the source sensor relayed the data to intermediate sensors until reaches the sink. This saves the energy and increases the network capacity, but also increases the difficulty of the routing.

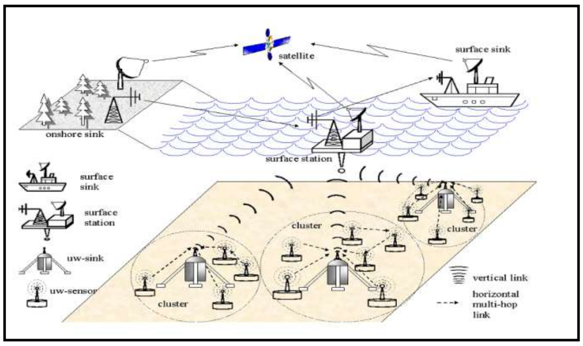


Fig. 3: Static two-dimensional UWSN [1].

3.2 Static Three-Dimensional Underwater Sensor Networks

Each node attached to a buoy by a cable. The sensed data transmitted to the central station by the buoy using RF signal. However, floating buoys may block ships navigating, or can be noticed and turned off by opponents in military applications. The scheme whose sensor nodes anchored to the bottom can overcome this. The sensors anchored to the seabed and fitted out with floating buoys. The buoy pays the sensor towards the water surface as in figure 4. The lengths of the cables are different for the required depth.

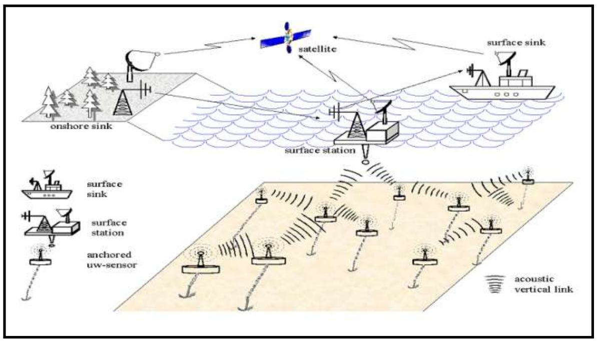


Fig. 4: Static three-dimensional UWSN (Node anchored to the bottom) [1].

3.3 Three-Dimensional with Autonomous Underwater Vehicles

It consists of lots of static sensors together with some autonomous underwater vehicles (AUVs), as shown in figure 5. AUVs play a key role for additional support in data harvesting. AUVs could considered as super nodes, which have more energy, can move independently, and it could be a router between fixed sensors, or a manager for network reconfiguration, or even a normal sensor. [7] proposes a specialized architecture for UWSNs to provide Energy Efficient and Robust Architecture.

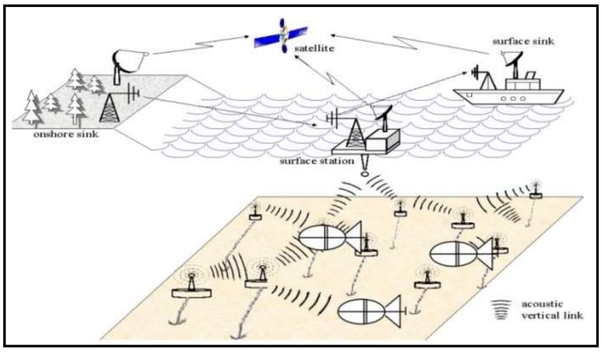


Fig. 5: Static three-dimensional with AUV [1]

4 UWSNs Applications

Applications of underwater networks fall into similar classifications as terrestrial sensor networks as follow [8]:

– Scientific applications: Which observe the environment from geological procedures on the seabed, to water characteristics (temperature, salinity, oxygen levels, bacterial and other pollutant content, dissolved matter) to counting or imaging animal life (micro-organisms, fish or mammals).

– Industrial applications: Which monitor and control commercial process, such as underwater tools related to oil extraction.

– Military and homeland security applications: Which include securing and monitoring port facilities or ships in foreign ports, and communicating with submarines.

– Shallow Water Acoustic Network for Mine Countermeasures Operations.

– Wireless Sensor Networks on the Great Barrier Reef.

– UASN for Early Warning Generation of Natural Events.

– Sensor Network Architectures for Monitoring Underwater Pipelines.

– Autonomous Underwater Surveillance Sensor Network (AUSSNet).

– Group-based UWSN for Marine Fish Farms.

– Underwater Acoustic Network for the Protection of Offshore Platforms and Energy Plants.

– SeaSTAR Underwater Monitoring Platform.

III. ROUTING PROTOCOLS IN UWSNs

The process of sending information from source nodes to a sink is a very challenging task especially in mobile nodes. Energy consumption is a principle objective. Beside that, node mobility is handled. Routing protocols divided into three categories proactive, reactive and geographical. Proactive or table driven effect a large overhead in order to create the routs, either periodically or every time when the topology modified. Reactive protocols are more appropriate for the dynamic networks, but they cause large delays and require the source to initiate flooding of control packets in order to create the paths. This makes both types of routing protocols unsuitable for UWSNs. Geographic routing considered the promising routing protocol for UWSNs. Geographical routing is a routing principle that relies on geographic position information. The geographic location of the destination receivespackets from the source instead of the destination network address [6]. Depending the serving nodes numbers,there are four possible scenarios which is all-for-some, some-for-some, some-for-all and all-for-all. Greedy, Restricted directional flooding and Hierarchical are the classification of these scenarios [9-11].

a) Greedy:-

It use the idea of know approximate location of the receiver and send the packet from source to it by optimized selection of next hop neighbour to the destination for example. VBF (Vector Based Forwarding), HH-VBF (Hob by Hop VBF), VBVA (Vector-Based Void Avoidance), ES-VBF (Energy Saving VBF), and CVBF (Clustering VBF Protocol) are some of the popular geographic routing protocols for UWSNs [10].

b) Restricted Directional Flooding:

It is based on selecting many next hop to the receiver by broadcasting the packet to neighbours which they decide if they are in the path to the receiver and continue to forward it or not and drop it. The focused beam routing (FBR) Directional flooding routing (DFR) and Sector-Based Routing with Destination Location Prediction (SBR-DLP) are the example for that [10].

c) Hierarchical:

It is used for moving node especially for large scale number of nodes. LCAD is an example for that [10].

1) Vector-Based Forwarding Protocol (VBF)

VBF is a source routed routing protocol where each packet carries routing information in its header. It uses the virtual pipe for routing principle and all the packets forwarded through it. Each packet contains three position fields, SP, TP, and FP, that is, the position of the source, the target, and the forwarder respectively. In addition, each packet contains RANGE field that controls the area where the packet flooded and RADIUS field that defines the radius of the routing pipe [12]. In figure 6, $\boldsymbol{S_1}$ is the source node, and $\boldsymbol{S_0}$ is the sink. The routing vector is$\overrightarrow{\boldsymbol{S_1 S_0}}$. Packets forwarded from $\boldsymbol{S_1}$to $\boldsymbol{S_0}$. Forwarders forms routing pipes are along the routing vector with a pre-controlled radius (the distance threshold W).

Upon receiving a packet, each node calculates the distance and angles of the signal to the forwarder. If a node decides that, it is near to the routing vector, it puts its own position in the packet (FP) and forwarding the packet. Otherwise, packets are dropped. The sensor nodes in the pipe are responsible for packet forwarding. Nodes, which are not near to the routing vector, do not forward. Routing in VBF is carried out by query packets in deferent ways:-

A. Sink Initiated Query

There are two queries types:

– Location-dependent query, the sink is interested in a specific area and knows the location of this area. The sink broadcasts an INTEREST query packet, which carries the information of SP and TP. The direction of this query is the targeted area following the pipe defined by SP and TP.

– Location independent query, the sink needs some particular kind of information without caring to its location. The sink issues the INTEREST packet carries invalid position for the target. This query will be overwhelmed to the objective area. Upon receiving such query, each node checks if the data sink needs is exist. If so, the node calculates its position and sends back the data packets needed to the sink. If not, it puts its position in the FP field and forwards the packet.

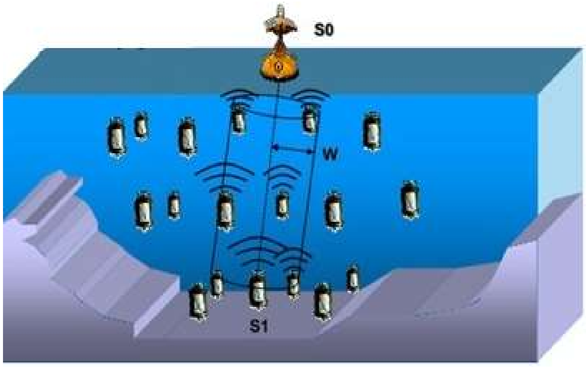


Fig. 6: Vector Based Forwarding (VBF) [1].

B. Source Initiated Query

Sensor node senses some events and wishes to notify the sink, it broadcasts a DATA READY packet. Upon receiving this packet, each node calculates its position and puts its position in the FP field and forwards the packet. When the sink receives such packet, it computes its position. Then it decides if it interests in such data. If so, source receives a location-dependent INTEREST packet.

Since the source node is moving, its location computed by the old INTEREST packet might not be true anymore. The source is sending packets to the sink and the sink makes use of the information of the source location carried in the packets to decide if the source is moving out from its interest location. If so, the SOURCE_DENY packet is sent from sink to stop this source from sending data. In the other hand, the sink initiates another interesting query to discover a new source.

1.1 Self-Adaptation Algorithm

All the nodes located within the routing pipe are capable to forward packets. In dense networks, many nodes might be concerned in the data forwarding. In order to save energy, it is necessary to regulate the forwarding based on the node density. It is infeasible to determine the node density due to the mobility. The self-adaptation algorithm allows each node to guess the density in its location and forward packets adaptively. This algorithm based on the definition of a desirableness factorα. This factor measures the compatibility of a node to forward the packet.

$$\alpha = \frac{P}{W} + \frac{R - d \times \cos\theta}{R}$$

– P is the projection length of node A onto the routing vector $\overrightarrow{S_1S_0}$.

– d is the distance between node A and F.

– θ is the angle between vector$\overrightarrow{FS_0}$ and vector $\overrightarrow{FA}$.

– R is the transmission range.

– W is the radius of the routing cannel.

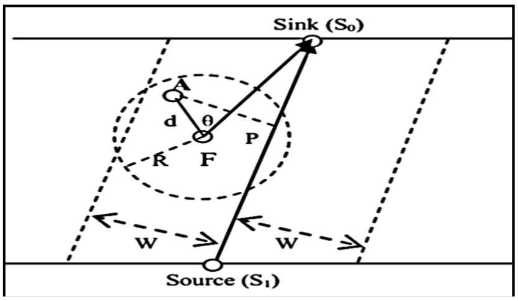


Fig. 7: Desirableness Factor [1].

When a node receives a packet, it determines if it is eligible for packet forwarding. If yes, the node waits a time interval $T_{adaptation}$then forwards the packets. This time interval based on the node's desirableness factor, a smaller desirableness factor, a less time to wait.

$$T_{adaptation} = \sqrt{\alpha} \times T_{delay} + \frac{R - d}{v_0}$$

– T_{delay}: A pre-defined maximum delay.

– v_0: The acoustic signals in water's propagation speed, 1500 m/s.

During the time period $T_{adaptation}$if a node receives the same packet from n other nodes, this node should calculate its desirableness factors relative to these nodes, and the original forwarder. If min $(\alpha_0, , \ldots, \alpha_n) < \alpha_c/2^n$ where α_c is a predefined initial value of desirableness factor ($0 \leq \alpha_c \leq 3$), then this node forwards the packet; if not, it discards the packet.

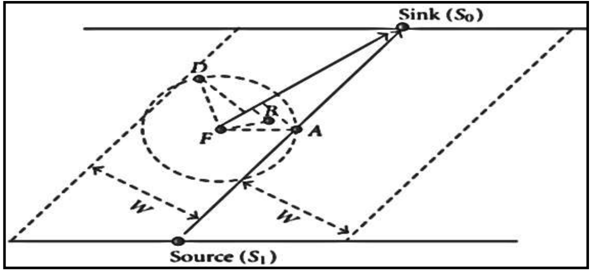


Fig. 8: Self-Adaptation Algorithm [12].

In figure 8, the node F is the present forwarder. There are three nodes, A, B, and D in its transmission range. Node A has the minimum desirableness factor. Therefore, A has the lowest delay, it sends the packet first. Node B discards the packet as it is exist in node A range. Node D is not in the transmission range of A. Thus, D also forwards the packet.

1.2 **Advantages of VBF**

– Reduces network traffic as only the nodes along the forwarding path are concerned in packet forwarding, hence saving the energy of the network.

– The packet delivery ratio increased in dense networks.

1.3 Disadvantages of VBF

- Sensitivity to the routing pipe’s radius.
- Small data delivery ratio in sparse networks.
- Multiple nodes acting as relay nodes in dense networks.
- Increase the communication time and energy consumption in dense networks.
- In case of a void, VBF cannot find a path to forward the packet.

2) Hop-by-Hop Vector-Based Forwarding Protocol (HH-VBF)

It based on the same idea of routing vector as VBF, therouting virtual pipe redefined to be a per-hop virtual pipe, instead of a single pipe from the source to the sink [13]. As we can see in figure 9, in HH-VBF, the impossible paths in VBF can be used here.

In HH-VBF the Self-Adaptation Algorithm is different from that in VBF. Each forwarder maintains a self-adaptation timer, which based on the desirableness factor. The timer defines the time the node waits before forwarding the packets.

2.1 The Self-Adaptation Algorithm

In HH-VBF, the desirableness factor determines a self-adaptation timer $T_{\text{adaptation}}$which is done in each forwarder. It is the time the packet be held before forwarding. The desirableness factor α' of a node A, is defined as

$$\alpha' = \frac{(R - d \times \cos\theta)}{R}$$

- d is the distance between node A and candidate forwarder F.
- θ is the angle between vector$\overrightarrow{FS_0}$ and vector $\overrightarrow{FA}$.
- R is the transmission range.

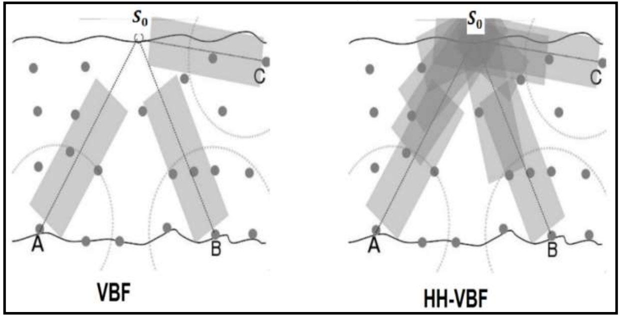


Fig. 9: VBF vs. HH-VBF [1].

The node with the lowest desirableness factor will forward the packet first. In this way, a node may hear the same packet multiple times. The node computes its range in various vectors from the packet received to the sink. If distance become more minimum but still higher than the pre-defined lower distance threshold β, this node will send the packet. if not, it discards the packet. The bigger β is the more nodes will forward the packet. So, adjusting β will control forwarding redundancy in HH VBF.

2.2 Advantages of HH-VBF:

- Less sensitive to the routing pipe radius than VBF.
- The packet delivery ratio increased in dense networks.
- Provide more paths to deliver data than VBF.

2.3 Disadvantages of HH-VBF:

- More packet overhead compared to VBF due to its hop-by-hop nature.
- Large propagation delay due to its hop-by-hop nature.
- High energy consumption in dense network.
- Can’t reach any node in case of a void.

3) Vector-Based Void Avoidance (VBVA)

Some areas of the network might not occupy with nodes (Void); VBVA extends the VBF to handle this problem. Initially, a routing vector is a path that sends data from source to target node. If void does not exist, VBVA acts the same as VBF. When there is a void, VBVA have tow mechanism which are: vector-shift mechanism or back-pressure mechanism, to be utilized [14].

3.1 Void Detection

Void can be detected by node when listening to neighbours nodes’ transmission of packets. For forwarding vector$\overrightarrow{\boldsymbol{ST}}$, and a node N, we define the advance of node N as the projection of the vector$\overrightarrow{\boldsymbol{SN}}$ on the forwarding vector$\overrightarrow{\boldsymbol{ST}}$. Void node is node which all neighbours’ advances are smaller than its own on sending data. In figure 10, the advances of nodes B, C and F denoted as $\boldsymbol{A_B, A_C}$ ***and*** $\boldsymbol{A_F}$. Node F hasgreater advances than all neighbours. Thus, node F is a void node [1]

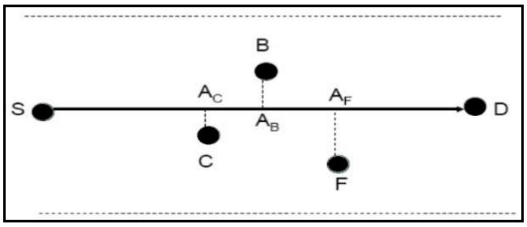


Fig. 10: Void Detection [6].

3.2 Vector-Shift Mechanism

At void case, node use vector-shift mechanism to overcome this problem. To do that, all neighbours receive a broadcast vector-shift packet. Every one of the node outside the present sending channel will attempt to forward the relating information packet taking after another sending vector from themselves to the objective. After shifting the forwarding vector of a packet, a node continues listening to the channel to check if there is a neighbour node advances the packet with the new sending vector. If the node does not hear that, the packet forwarded even if it shifts the current forwarding vector, the node defined as an end node. For an end node, the back-pressure mechanism is used instead of the vector-shift mechanism [1].

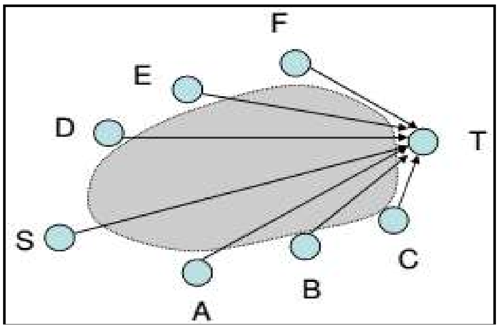


Fig. 11: Vector-shift mechanism [1].

In figure 11, the dashed area is a void area. Source node isS and Target node is T. S send the packet through the vector $\overrightarrow{ST}$ then it keeps listening to the channel for some time. Since the neighbor node, D and A of S are not within the transmission channel, they will not send the packet. Node S cannot hear any transmission so it is across void. It broadcasts a vector-shift control packet toneighboursasking to find out alternative vector to $\overrightarrow{DT}$ and$\overrightarrow{AT}$, nodes D and A repeat the same process [1].

3.3 Back-Pressure Mechanism

Back-Pressure (BP) packet is a broadcast packet from node becomes an end node. Upon receiving this control packet, each neighbouringnode tries to move the sending vector in the event that it has never moved the sending vector of this packet before. Otherwise, the node telecasts the BP packet once more. The BP packet will be routed back in the direction moving away from the target until it reaches a node which can do vector shifting to forward the packet toward the target [1].

In figure 12, the dashed area is a void area. Source node is S and target node is T. When S forwards the packet with forwarding vector $\overrightarrow{ST}$to node C, sincenode C can't send the packet through the vector $\overrightarrow{ST}$any more. It will first use vector-shift mechanism to discover optionroutes for the information packet. Since node C is an end node, it cannot catch the transmission of the packet. Node C then use BP packet broadcast. After receiving the BP packet, node B first tries to move the forwarding vector but fails to find routes for the data packet. Then node B broadcasts BP packet to node A and so on. Finally, a BP packet routed from node A to the source S. Node S then shifts the forwarding vector to $\overrightarrow{DT}$and$\overrightarrow{IT}$. The data packet is sent to the destinationusing the vector-shift from nodes D and H [1].

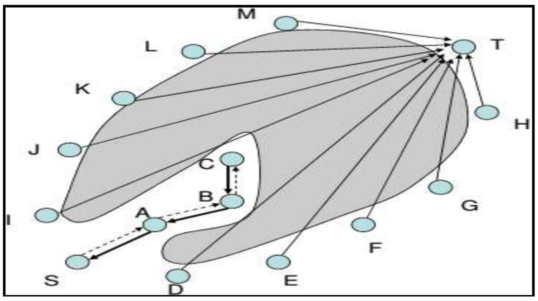


Fig. 12: Back-pressure mechanism [1].

3.4 Advantages of VBVA

– Solve the void problem.

– Void avoidance mechanism generates multiple forwarding vectors, which improve the robustness of the network.

3.5 Disadvantages of VBVA

– VBVA void avoidance mechanism introduces more energy consumption.

– More signalling overhead generated by void avoidance mechanism.

– Large propagation delay in case of presence of voids.

4) Energy Saving VBF Protocol (ES-VBF)

ES-VBF introduces node's energy information into VBF protocol. The routing process considers both factors of position and energy consumption [15]. VBF algorithm only considers location information to transmit data packet. However, when there is a node whose location is always the best in routing pipe, it will be selected again and again during routing selection. Thus, the energy of this node exhausted, causing routing failure. ES-VBF adds the value of energy consumption into desirableness factor to decide waiting time. Improved desirableness factor α:

▪ If Node residual energy is larger than 60 % of initial energy:

$$\alpha = \frac{P}{W} + \frac{R - d \times \cos\theta}{R}$$

▪ If the Node residual energy is smaller than 60 % of initial energy:

$$\alpha = 0.5 \times \left(1 - \frac{\text{energy}}{\text{initialenergy}}\right) + \frac{P}{W} + \frac{R - d \times \cos\theta}{R}$$

− energy : The residual energy of node.

− initialenergy: Initial energy of node.

Waiting time $T_{\text{adaptation}}$ is inversely proportional to residual energy. Nodes with higher residual energy have smaller desirableness factor, higher priority of forwarding packets and shorter waiting time among neighboring nodes.

4.1 Advantages of ES-VBF

– Reduces energy consumption of network compared to VBF.

– Balance the network energy consumption compared to VBF.

– Prolong the lifetime of network.

4.2 Disadvantages of ES-VBF

ES-VBF has all the disadvantages of VBF routing protocol.

– Sensitivity to the routing pipe's radius.

– Cannot handle the void problem.

– Not suitable in sparse network.

– Multiple nodes acting as relay nodes in dense networks.

5) Clustering Vector-Based Forwarding Protocol (CVBF)

The whole network divided into a predefined number of clusters. All nodes assigned to the clusters based on their geographic location. One node at the top of each cluster selected as a virtual sink. The rest of nodes in each cluster transmit the data packets to their respective cluster virtual sink. The routing inside each cluster follows the VBF routing protocol. CVBF defines one virtual routing pipe for each cluster, instead of one virtual routing pipe for all network nodes in VBF. The routing pipe radius is equal to the transmission range of a node. After receiving the data packets from the sensor nodes, cluster virtual sinks perform an aggregation function on the received data, and transmit them towards the main sink using single-hop routing. Cluster virtual sink nodes are responsible for coordinating their cluster members and communicating with the main sink [1, 16]. The algorithm stated in the following steps:

5.1.1 Step1: Clustering the Nodes

The network divided into groups of nodes according to their geographic location producing non-overlapping clusters excluding the main network sink, which allocated on the water surface. The network space divided into equal space volumes in the form of cuboids as shown in figure 13.

The division based on the values of X and Y coordinates, and the cluster widthcw. Choosing the best number of clusters as:

$$N = \frac{X \times Y}{(cw)^2}$$

– $X \times Y$: The total surface area of the network

– cw: The area of the cluster surface.

The choice of N that gives the value of cw as near as possible to $\sqrt{2}R$ to make sure that the virtual pipe of the cluster includes all the nodes inside that cluster.

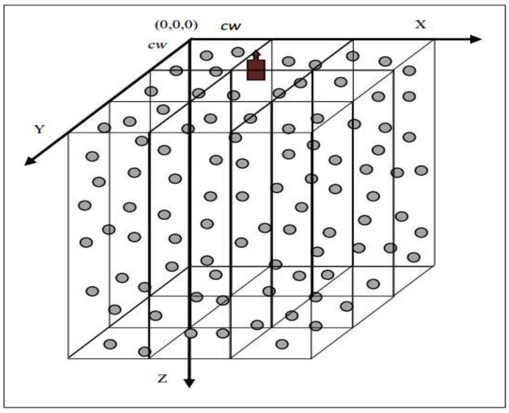


Fig. 13: CVBF network area with clusters [1].

5.1.2 Step2: Selecting the Cluster Virtual Sink

For each cluster, which has a space volume cw×cw×Z, choose the node, which is nearest to the main sink to be a cluster virtual sink. If more than one node has the same depth position, we choose the nearest node to the cuboid's axis, in which its surface point coordinates is the point (X_c,Y_c, 0). The source node of the cluster is fixed at the position (X_c,Y_c,Z_{max}). All other nodes can send data to their corresponding virtual sink following the mechanism of VBF and depending on the value of its desirableness factorα.

$$X_c = \frac{X_{max} - X_{min}}{2}, Y_c = \frac{Y_{max} - Y_{min}}{2}.$$

5.1.3 Step 3: Calculating the Cluster's Maintenance Time

This step takes into consideration the node mobility that affects network topology and performance. The maintenance algorithm executed simultaneously in all clusters. In this step, a suitable periodical time called maintenance time T_m. Each node in the cluster checks its belonging to that cluster after T_m. If a node belonging to a cluster moves away from that cluster, it naturally has two choices. The first choice is to enter another cluster. The second choice is that it exits from all the network volume. To avoid exiting a node from the network volume, the node positions have to be carefully choosing far from the network space boundaries.

$$Tm = \frac{d_{max}}{S}$$

– d_{max}: Maximum distance of a node movement.

– S: The current speed of the node.

5.2 Advantages of CVBF:

By studying CVBF protocol, we observe that it has some advantage as:

– Overcome the pipe sensitive radiuses of VBF.

– Has high packet delivery ratio compared to VBF.

– Data delivery ratio in sparse networks is higher than VBF.

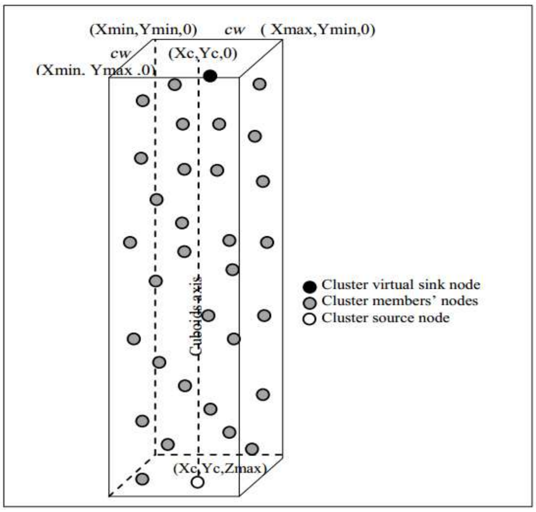


Fig. 14: One cluster and its virtual sink [1].

5.3 Disadvantages of CVBF:

We notice that it has some drawbacks as:

- Virtual sink nodes consume more power when compared to others nodes of the same cluster.
- Failure of virtual sink nodes will lead to untimely shutdown of its cluster's nodes.
- Cannot handle the void problem.
- CVBF clustering mechanism causes processing overhead.
- The protocol handling the node mobility using T_m however, it did not explain a technique that handles the virtual sink mobility "for how long the node act as a virtual sink, and in case of another node closer to the main sink and cuboid's axis than the current virtual sink".
- No energy balance consumption in the network duo to the asymmetric nodes distribution among clusters.

6) Reliable and Energy Balanced Algorithm Routing (REBAR)

It is a location based routing protocol which deals with three main issues concerned in UWSNs: saving energy, delivery ratio and resolve void. To test energy consumption, Itutilizes a sphere energy depletion model.Then it gets use of node's mobility to prolong lifetime of network by balance the consumption. Constant rate and matchless ID are assigned to each node. There are some assumptions to be taken in consideration.

• Node's location and destination are predefined.
• Transmitted data is done by certain rate [10].

7) The Focused Beam Routing (FBR)

Location and final receiver are assumed to be known to each node. It use different level power which corresponding to transmission radius.It provide tool to avoid broadcast. It is suitable for network consists of both static and mobile node awareness of other node's location is not necessary [10].

8) Directional Flooding Routing (DFR)

It focuses on node mobility and water conditions and considers link quality strategy of forwarding. In this protocol, location of node, next hop, sink and geographic information are assumed to be known. Nodes can calculates link quality with neighbours. DFR also solve the void problem. It uses a scoped flooding [10].

9) Location Aware Source Routing (LASR)

Here,link quality metric and location awareness are handled. All data about routing are mentioned in packets' header which make header size is larger and increase as long as the hope increased [10].

10) A Sector-Based Routing with Destination Location Prediction (SBR-DLP)

It is based on knowing its location and predication the location of destination. Information about the neighbour is not necessary.The destination node's location is pre-planned movements.From candidate neighbour, node chooses the next hop.It looks into the whole correspondence communication circle to locate the candidate node [10].

11) LCAD

It is a clustering algorithm. It divides all networks into 3D grid which has the size of 30m x 40m x 500m. The data communication is classified into three steps: (i) set-up. (ii) Data gathering phase. (iii) Transmission phase. the sleep wake pattern use to choose cluster header along with residual memory and energy of the contending Ch-nodes [10].

12) Information Carrying Routing Protocol (ICRP)

ICRP makes use of control packets that are carried by data packets. ICRP does not incorporate the use of state or location information, and also only a small fraction of the nodes participate in the routing process. The ICRP incorporates three steps that are, route finding, route preservation and route renunciation.

13) Depth Based Routing Protocol (DBR)

DBR needs just the depth information of sensor nodes. DBR is a desirous algorithm that tries to direct a packet from a source node to sinks to acquire the depth of current node; each sensor node is outfitted with a reasonable depth sensor. DBR utilizes the various sink construction modeling as a part of which different number of sinks are put on the water level and are utilized to gather the information packets delivered by the sensor nodes. DBR takes the routing decision on the basis of depth data, and advances the information packets from higher depth nodes to lower depth sensor nodes.

14) Hop- by- Hop Dynamic Address based Routing Protocol (H2H-DAB)

Sensor nodes utilize the dynamic address to get new delivers as indicated by their new positions at distinctive depth levels. This convention utilizesnumerous surface buoys that are utilized to gatherinformation and a few nodes are secured at bottom and the rest of the nodes are tied down at diverse depths. Nodes closer to the surface have smaller value of addresses, and these addresses get to be bigger as the nodes travel towards the bottom. In first stage, it assigns the dynamic addresses to the sensor nodes, and in second stage, information is sent utilizing these addresses. With the assistance of hello packets, dynamic addresses are assigned to nodes and these addresses are produced by the surface sinks.

15) Constraint Based Depth Based Routing Protocol (CDBR)

The sensor nodes are sent under the water haphazardly. Various sinks are sent on the sea level whereas the sensor nodes are in charge of conveying the sensed information to the sinks. RF modems and Acoustic modems are the major parts of the sinks. The sensor nodes under the water are furnished with Acoustic modems. The nodes correspond with one another and the Sinks utilizing the Acoustic Modems. The sinks correspond with one another and the on-shore server farm utilizing the RF Modems. Information arriving at any of the sinks is considered as information conveyed effectively.

16) Mobile Delay-Tolerant Approach (DDD)

It uses collector nodes called dolphins to gather information that is sensed by the sensor nodes. The recommended scheme shuns multi-hop communication, and data is sent to acoustic nodes that are in its communication range. The sensors occasionally wakeup to sense data and to generate some events. The acoustic modem is centered on two parts. The first part is utilized for acoustic communication with the close dolphin, and the other part is to use small power device to find out the happen of dolphin nodes and the activation of the first component is done through this.

17) Performance Comparison of UWSNs Routing Protocols

Design a routing protocol is a challenging task. All the nodes inside UWSN should be reachable (Connectivity) while covering process (Coverage), even when the nodes inside the network start to fail due to energy issues or other problems (Fault Tolerance). The protocol should also adapt network size and density (Scalability) and provide a certain QoS. In parallel way, designers must tryto use the memory and energy consumption of the protocol efficiently.

We compare between all the surveyed routing protocols according to our studies and other related works [17]. Factors such as the number of nodes in the network affects matters of data pack delivery, end-to-end delay and energy consumption. Thus, we compare between these protocols with respect to spares and dense networks. Table 2 summarizes the comparison results for VBF's protocol. Table 3 elaborates the comparison between protocols in point of view of their characteristics. Performance comparison is mentioned in Table 4. Table 5 monitors the metrics of protocols where Table 6 discusses the application and advantage and disadvantage of each protocol.

VI. SECURITY IN UWSNs

UWSNs used in various fields of interest withincreasing need for security. This need for security appeared in case of military applications or applications working with sensitive data. Compared to the research in security for WSNs, UWSN security research is limited. Achieving security objectives in UWSNs is a challenging task due to the special constraints of underwater environment. Nodes have limited processing capability, very low storage capacity, limited bandwidth, and limited energy. Therefore, security services in UWSN should protect the information over the network and take into account the limited resources of the nodes.

1) Security Requirements

In order to achieve security in UWSNs, security requirements should be provided [3, 5, 18]. These security requirements represented in Table 7.

2) Security Threats

UWSNs are susceptible to security attacks because of the broadcast nature of the transmission medium. Moreover, UWSNs have an additional vulnerability because nodes not physically protected. Attackers may do various types of security threats to make the UWSN system unstable [18]. A useful means of classifying security attacks is in terms of passive attacks and active attacks.

2.1 Passive Attacks

The goal of the adversary is to obtain the information that is being transmitted. No alteration of data makes passive attack difficult to detect. Passive attacks are also known as Attacks against Privacy. There are some common attacks against privacy are:

Monitor and Eavesdropping: an adversary could eavesdrop and intercept transmitted data. To prevent these problems we should use strong encryption techniques.

Traffic analysis attacks: the attacker predict the nature of communication by captures the packets in order to analyse the traffic, determines the location, identifies communicating hosts, and observes the exchange of the message. Using all these information, they predict the nature of communication.

2.2 Active Attacks

It involves modification or creation of a false packet. The adversary able to control all the data sent. There are some common active attacks are:

- Modification: The adversary can simply intercept and modify the packets' content.

- Replay: The adversary re-transmits the contents of the packets later.
- Injection: the attacker sends out false data into the network.

An attacker compromises the sensor by different ways, gains control or access to the sensor node itself. Attackers can physically breaking into the hardware by modifying its hardware structure, or by taking the data from the hardware device without any form of hardware structural modification. The compromised node then behaves in some malicious ways, e.g., to generate a fake message and to attack the network. Complex attacks from compromised nodes can target the internal protocols used in the network, such as routing protocols. Vulnerability of routing protocols is usually caused by missing authentication, freshness and integrity check of the routing information. This fact is denoted in the following attacks:

Table 2: Comparison among VBF routing protocols.

		VBF	**HH-VBF**	**VBVA**	**ES- VBF**	**CVBF**
Cluster Head						✓
Handle void				✓		
Suitable to be implemented in	**Dense**	✓			✓	✓
	Sparse		✓	✓		
Network design	**Mobile Nodes**	✓	✓	✓	✓	
	Static Nodes	✓	✓	✓	✓	✓
Robustness	**Dense**	High	High as VBF	High as VBF More robust than VBF & HH-VBF in void presences	High as VBF	High as VBF Low in case of virtual sink failure
	Sparse	Low	More robust than VBF	Low as VBF	Low as VBF	Low as VBF
Single/Multi Sink		Single	Single	Single	Single	Single virtual sink per cluster
Forwarder node criteria		Distance	Distance	Distance	Distance/ energy	Distance
Sinks deployment		One fix on surface	One fix on surface	One fix on surface	One fix on surface	Multi virtual /one fix on surface
Forwarding Shape Region		Single pipe routing	Per-hop pipe routing	Single pipe routing / Multiple pipe routing in case of void presences	Single pipe routing	Single pipe routing per cluster
Sensitivity to routing pipe radius.		High sensitive	Less sensitive than VBF	Not sensitive	High sensitive as VBF	Not sensitive
Data Delivery Ratio	**Dense**	High	High	High	High	High
	Sparse	Low	Higher than VBF	Higher than VBF & HH-VBF	Low	Low
Energy Consumption	**Dense**	High	Higher than VBF	High as VBF High in void presences	Less than VBF	High as VBF
	Sparse	Low	Higher than VBF	Low as VBF	Low as VBF	Low as VBF
End to End Delay	**Dense**	Low	Higher than VBF	Low as VBF	Higher than VBF	Low
	Sparse	High	Less than VBF	Less than VBF & HH-VBF	High as VBF	High as VBF

Table 3: Comparison of routing protocols based on their characteristics [19].

Protocol/ architecture	Single/ Multiple copies	Hop-by-hop/ end-to-end	Clustered/ single entity	Single/multi-sink	Hello or control packets	Requirements and assumptions	Knowledge required/ maintained	Remarks
VBF	Multiple	End-to-end	Single-entity	Single-sink	No	Geo. location is available	Whole network	Considered as first geographic routing approach for UWSN
HH-VBF	Multiple	Hop-by-hop	Single-entity	Single-sink	No	Geo. location is available	Whole network	Enhanced version robustness improved by introducing hop-by-hop approach instead of end-to-end
FBR	Single-copy	Hop-by-hop	Single-entity	Multi-sink	Yes	Geo. location is available	Own and sink location	A cross layer location-based approach, coupling the routing, MAC and phy. layers.
DFR	Multiple	Hop-by-hop	Single-entity	Single-sink	No	Own, 1-hop neighbors and sink info	Own and sink location	A controlled packet flooding technique, which depends on the link quality, while it assumed that, all nodes can measure it
REBAR	Single-copy	Hop-by-hop	Single-entity	Single-sink	No	Own, 1-hop neighbors and sink info	Own and sink location info.	use adaptive scheme by defining propagation range. Water movements are viewed positively
SBR-DLP	Single-copy	Hop-by-hop	Single-entity	Single-sink	Yes	Geo. location is available	Own location and sink movement	does not assumes that destination is fixed plus it consider entire communication circle instead of single transmitting cone
DDD	Single-copy	Single hop	n/a	n/a	Yes	Network with special setup	About dolphin node presence	A sleep and wake-up scheme, which requires only one-hop transmission
DBR	Multiple	Hop-by-hop	Single-entity	Multi-sink	No	Nodes with Special H/W	No network information maintained	Considered 1st depth based routing. After receiving data packet, nodes with lower depth will accept and remaining discards
H2-DAB	Single-copy	Hop-by-hop	Single-entity	Multi-sink	Yes	n/a	1-hop neighbor's	Short dynamic addresses called Hop-IDs are used for routing, assigned to every node according to their depth positions
LCAD	Single-copy	Hop-by-hop	Clustered	Single-sink	Yes	Nodes with special H/W	Own cluster information	Clusters are formed, in order to avoid multi- hop communication
LASR	Single-copy	End-to-end	Single-entity	Single-sink	Yes	Network with special setup	Source to sink information	A DSR modification. Location and link quality awareness is included. Preferred only for small networks

Table 4: Performance comparison of UWSN protocols [19].

Protocol / architecture	Delivery ratio	Delay efficiency	Energy efficiency	Bandwidth efficiency	Reliability	Cost efficiency	Performance
VBF	Low	Low	Fair	Fair	Low	n/a	Low
HH-VBF	Fair	Fair	Low	Fair	High	n/a	Fair
FBR	Fair	High	High	Fair	Fair	n/a	High
DFR	Fair	Fair	Low	Fair	High	n/a	Fair
REBAR	Fair	Low	High	Fair	Fair	n/a	Fair
DDD	Low	Low	High	Fair	Fair	Low	Low
DBR	High	High	Low	Fair	High	Fair	High
H2-DAB	High	Fair	Fair	Fair	Fair	High	Fair
LCAD	Fair	Low	Fair	Fair	Low	Low	Low
LASR	Fair	Low	Fair	Fair	Fair	High	Fair

Table 5: Metric comparison of UWSN protocols [9].

Parameter and Protocol	Localization of nodes required	Multi-sink architecture	Technique used	Basic parameter onto which routing decision is made	Network topology	Control packets	Routing table required
ICRP	No	No	Broadcasting	Path life- time	Dynamic	Yes	Yes
DFR	Yes	No	Packet flooding	Base angle or criterion angle	Dynamic	No	Yes
DBR	Only depth information	Yes	Broadcasting	Depth of neighbor	Static	No	Yes
CDBR	Only depth information	Yes	Broadcasting	Depth threshold value	Static	No	Yes
H2- DAB	No	Yes	Dynamic addressing	Dynamic address	Dynamic	Yes	No
VBF	Yes	No	Virtual routing pipe	Node nearer to the virtual pipe	Dynamic	No	Yes
SBR-DLP	Yes	No	Multicasting	Distance to destination node	Static	No	Yes
DDD	No	Yes	Broadcasting	N/A	Static	Yes	No
LASR	Yes	No	Link quality metric and location awareness	Shortest path metric	Local	No	Yes

Table 6: Comparison of routing protocols in UWSN [20]

Routing protocol	Category	Application	Advantages	Disadvantages
VBF **HH-VBF** **FBR** **REBAR** **SBR-DLP** **DFR LASR**	Location based routing	Energy-efficient UASN	a) Energy efficient b) Robustness c) High success of data delivery	a) Low bandwidth b) High latency c) Delay efficiency, ,performance and reliability are low
DBR	Depth based routing	Dense network application	a) Very high packet delivery ratio b) No need of full dimensional location information of nodes	a) Not energy efficient b) Batteries are stranger to recharge
LCAD	Cluster based routing	Energy-efficient UWSN	a) High scalability and robustness b) Less load and energy consumption	a) Processing overhead is complex

Table 7: The security requirement of UWSNs [3, 5, 18].

Security Requirement	**Definition**
Authentication	Verifying that communicating nodes are who they claim to be. It can be achieved by Massage Authentication Code (MAC)
Confidentiality	Hiding the data from everyone except for those who are authorized. It can be achieved by the use of encryption.
Integrity	Ensures that the packet is not altered during transmission.
Availability	Guarantee to provide the network services even when the system is attacked.
Non-repudiation	Prevents the source to deny that it sent that packet.
Freshness	To be sure that there is no old massage resent again.
Secure Localization	The ability to localize each sensor. Localization can help in making routing decisions, so the attackers are searching the header of packet. The secure localization is an important factor during implementing security in the network. It can be achieved by encrypting the header of the packet.
Self-Organization	Distributed sensor networks must self-organize to support multi-hop routing. Such self-organization is hard to be securely done.
Secure Time Synchronization	Time synchronization is very important for many operations, such as coordinated sensing tasks, and sensor scheduling (sleep and wakeup).
Robustness and Survivability	The UWSN should stand against different security attacks, and if an attack success, then its effects should be negligible.

2.2.1 Sinkhole Attack

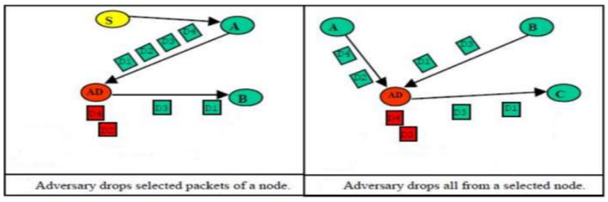
The goal of this attack as monitored in figure 15, is to pull in as much of the traffic as possible to the deceived node. The adversary places malicious node to the closest sink. The deceived node tries to look very popular to other nodes in point view of the routing algorithm. The result is that the neighbor nodes choose the compromised node as the next-hop node to route their data through. Authentication of nodes exchanging routing information or redundant paths can defense this attack

2.2.2 Selective Forwarding Attack

An attacker may create malicious nodes which selectively forward only certain messages and simply drop others. In UWSNs it should be confirmed that the receiver is not receiving the information due to the attack and not because it located in a shadow zone. Multi-path routing can effectively defense these attacks However, multipath routing increases communication overhead. Another solution of this attack is to check the sequence number of the data packet. It is shown in figure 16.

2.2.3 Sybil attack

In figure 17, an advanced version of an impersonate attack, in which an attacker can forge identities of nodes by appearing in multiple places at the same time. Geographical routing protocols are also vulnerable because an adversary with several identities can claim to be in multiple locations at once. Authentication and position verification are methods to protect against this attack, while position verification is difficult in UWSNs due to the mobility.



Adversary drops selected packets of a node.

Adversary drops all from a selected node.

Fig. 16: Selective Forwarding attack in UWSNs.

2.2.4 Homing Attack

Some nodes may have special responsibilities, such as sink node and cluster-head node. These nodes attract malicious attacker's interest. He tries to block the normal function of these nodes. Once these nodes failed or compromised, the whole or a portion of the network might become useless. Location based forwarding protocols expose to such attack. The attacker passively listens to the network and learns the location of such nodes. Then these nodes are attacked and brought down. One approach is to encrypt the packets headers to hide the location of the important nodes.

2.2.5 Wormholes Attack

Two malicious nodes cooperate by tunneling packets to establish shortcut appearance using private communication channel which lead to increase the probability of being selected path. Then, it drop packet and analysis traffic. Routing protocols choose the paths that hold wormhole links because they seem to be shorter. Location based protocols can also be vulnerable to this attack when malicious nodes claim wrong locations and mislead other nodes. It is elaborated infigure 18. A general solution for detecting and countering wormhole attacks based on packet leashes. Two types of packet leashes introduced namely temporal and geographical leashes.

2.2.6 Jamming Attack

Sending unwanted signal that may corrupt the packet which lead to high error rate and low performance. Most common defense against jamming attacks is to use spread spectrum techniques and switching nodes to a lower duty cycle hence, preserving power.

2.2.7 Tampering

An attacker can damage or modify nodes physically. Due to underwater nodes may be deployed in enemy zone and the network may consist of hundreds of nodes spread large scales, we cannot ensure the safety of all nodes. An attacker may compromise nodes to read or modify its internal memory. Traditional physical defenses include hiding nodes.

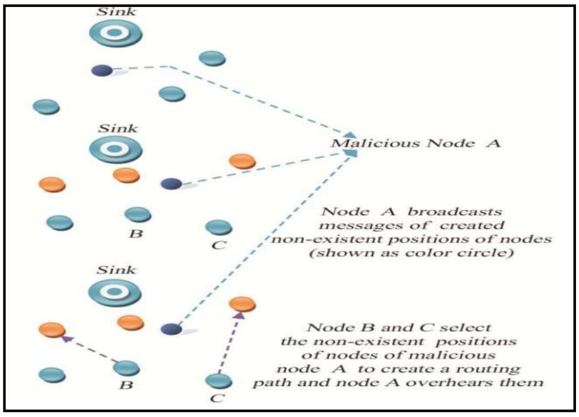

Sink
Sink
Sink
Malicious Node A
Node A broadcasts messages of created non-existent positions of nodes (shown as color circle)
B
C
Node B and C select the non-existent positions of nodes of malicious node A to create a routing path and node A overhears them
B
C

Fig. 17: Sybil attack in UWSNs.

2.2.8 Acknowledgment Spoofing

A malicious node catching packets sent to its neighbor nodes used to hoodwink link layer acknowledgments with the objective of strengthening a weak link which is situated in a shadow zone. Shadow zone is a distributed routing protocol and these are formed when the acoustic rays are bent and sound waves cannot pass into the network which can cause high bit error rates and loss of connectivity in the network. Counter measure are: Encryption of all packets sent through the network.

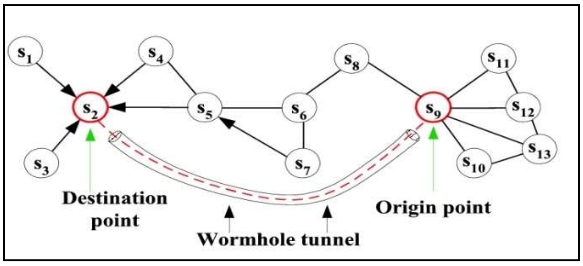


Fig. 18: Wormholes attack in UWSNs.

2.2.9 Hello Flood Attack

A malicious node send a hello packet that may translate the false presumption about the attacker is a neighbor and the node will accept that the neighbor node is inside the radio range and forward every one of the packets to the malicious node. The transmission power is very high for adversary node when compared with the other nodes in the network. Bidirectional connection verification method can secure against this attack, however it is not precise due to mobility of the nodes and the high propagation delays of UWSNs. Authentication is also a possible defense. It can be overcome using following two techniques are: 1. Bidirectional link verification. 2. Authentication in a possible defense.

3) Security Comparison

UWSN security is a critical issue to consider when designing network system. Due to data theft, data changes, energy and cost consuming, a secure environment to rout data becomes one of the essential needs. However, the surveyed routing protocols designed without the consideration of security issues. A comparison of different attacks on the surveyed routing protocols of UWSN based on their nature and goals is given in Table 8.

The surveyed protocols are Location-based routing protocols and they based on the broadcast nature of the acoustic channel which make them vulnerable to security attacks, given that packet information can be overheard by passive intruders or unauthorized nodes. In other hand, this Location-based technique increases the concerns of securing the location information, which included in each data packet transmitted. Moreover, since no governing mechanism exists to verify that a node is in fact at the position it is claiming, malicious attackers can easily exploit the system. Furthermore, the holding time, used to schedule the forwarding of data packets, allows malicious attacker to exploit these protocols and implement various routing disruptions on the network. Table 9 summarizes all the surveyed security attacks, including the attack name, a brief description, and possible solutions.

V. SIMULATION AND MODELING TOOLS

1) Simulation Tools

UWSN use acoustic signal to communicate due to the lack performance of radio signal in underwater. Testing new protocol is more appropriate using simulation tool. A Number of advantages are like inexpensive, implemented, and scalable. Table 10 summarizes the simulation programs and its characteristic. Each simulator isperfect for certain application rather than the others.The tool, which is called an emulator, is simulator usehardware. It getsbenefits from software and hardware to apply several scenarios in the same time [21].

Table 8: Security analysis among routing protocols [3].

Threats	Condition	Reason
Selective Forwarding	All protocols are secure against it.	Because, all packets exchanged based on flooding technique. However, in case of sparse network and void nodes, all protocols are vulnerable except VBVA.
Sybil Attack	All protocols are vulnerable to it.	Because, there is no authentication mechanism uses by nodes and there is no guarantee that a node is in fact at the position it is claiming.
Sinkhole Attack	All protocols are secure against it except CVBF.	Because, all packets exchanged based on flooding technique. However, CVBF would be vulnerable to it, in case of the malicious node placed close to the virtual sink node.
Homing Attack	All protocols are secure against it except CVBF	Because, there is no special-purpose nodes except in CVBF i.e. Virtual Sink node.
Eavesdropping	All protocols are vulnerable to it.	Because all packets broadcasted without using any encryption mechanism.
Jamming	All protocols are vulnerable to it.	Because all packets broadcasted in a shared communication channel. Thus, an adversary can inject unwanted signals into this communication channel.
Tampering Attacks	All protocols are vulnerable to it.	Because the deployment of the nodes is on an open /dynamic /hostile environment thus, physical access, capture and node destruction could be done.

Table 9: Brief description of security attacks and its countermeasures [3].

Attack	Description	Countermeasure
Sinkhole	The adversary places malicious node to the closest sink. The malicious node becomes very popular to other nodes.	Multipath and authentication of nodes exchanging routing information.
Selective Forwarding	Inducing the nodes to route the traffic through a set of compromised nodes, which then drop the routed packets.	Supporting multipath and authentication of nodes exchanging routing information.
Sybil	Malicious node impersonates some nonexistent nodes; it will appear as several malicious nodes with multiple identities.	Authentication and position verification.
Homing attack	An attacker achieves DoS against the special purpose nodes. Once these nodes failed the whole network become useless.	Hiding and Encryption.
Wormhole	Two malicious nodes directly connected, receive packets at one node and tunnels them to the other node. This creates a man in the middle attack and dropping the packets.	Packet leashes.
Jamming	The jammer determines the frequency of communication then injects unwanted signals into the communication channels.	Spread spectrum, lower duty cycle, and mapping the jammed area in the network and routing around it.
Tampering	An attacker tries to damage or modify the nodes physically.	Traditional physical defenses include hiding nodes.

A) NS-2

It was designed by Defence Advanced Research Projects Agency (DARPA) and National Science Foundation. It handles both wire and wireless networks. It is an open source programme. Tool Command Language (TcL) is used for simulation code. It has many features for sensor networks scenarios [21].

Merits:

1. Supportsvarious protocols.
2. Inexpensive.
3. Easily to remote modified.

Demerits:

1. Difficult command language.
2. Complicated
3. long run-time
4. There is no GUI.

B) EmStar

EmStar is an Emulator particularly planned for WSN. It is used as simulator and emulator. It has variable services and functions for wireless systems [21].

Merits:

1. Flexible.
2. Easy to evaluate faults and error
3. Robustness.
4. Good handle to debug

Demerits:

1. Lowerrange to be scalable
2. Decrease reality of simulation

C) GloMoSim

Global mobile Information System Simulator (GLoMoSim) has various wire and wireless networks. It can execute using a different synchronizing protocols, based on equal shared memory and distributed memory computers. It simulates wireless networks [21].

Merits:

1. Scalable.
2. It provides protocols for adhoc networking.
3. Handle mobility.

Demerits:

1. Simulate only wireless networks
2. Lower efficiency
3. No routing protocol
4. Hard to handle large networks.

D) Shawn

It is an open source. It can be written in Java. It provides tools to implement easily. Nodes can communicate easily using communication model [21].

Merits:

1. Handle dense protocol.
2. Channel Parameters' effect can be detected.

Demerits:

1. limited simulation parameter.
2. Limited code language.

E) UWSim

It is primarily for USN. It handles some special scenarios like low-bandwidth, high transmission,low frequencyand limited memory [21].

Demerits:

1. Lower functionalities.
2. Low number of scenarios.

F) VisualSense

It is a component-based structure. It provides scalableradio model

Demerits:

1. Only protocol of sound.

G) JSim

It is based on the concept of autonomous component architecture (ACA). It has a GUI library. You can also usescript interfaces that integrate with different code languages such as Perl, Tcl or Python [21].

Merits:

1. High performance.
2. Independent platform
3. Memory availability.

Demerits:

1. hard to handle.
2. long run-time.
3. difficult to use.

H) OMNeT++

It is a framework and use to write a simulation [21].

Merits:

1. GUI is Powerful.
2. Simulator is easier
3. Simulate power consumption problems in WSN
4. Support MAC protocol.

Demerits:

1. Limited protocols.
2. Incompatible problem.
3. Higher bugs

I) Aqua-Sim

It can simulate the attenuation and data loss in UWSNs. It has a compatibility with NS-2. the CMU wireless simulation packages is compatible with it. It is not affected by any wireless simulation package and don't affect other package in case of any modification to it. It is flexible. Entities, Interfaces and Functions are the basic classes [22].

Merits:

1. Discrete-event driven network simulator
2. 3D networks besides mobile networks are supported.
3. High fidelity simulation for underwater acoustic channels.
4. Easily import new protocols

Demerits:

1. In underwater, acoustic signals are very slow.

J) QualNet

QualNet is a comprehensive tool which simulates the real communication network. It has a full function to animate all scenarios. Graphical tool is existing and provide various options to monitors the scenarios. It provides real-time speed to allow software-in-the-loop. It can be used for a cluster, multi-processor systems andmulti-core [21].

Merits:

1. Extensibility.
2. Outstanding speed.
3. Ability to recallable.
4. Flexible model for higher numbers of nodes.

2) Modeling Tools

Modeling is a representation of a system that allows for investigation of the properties of the system and, in some cases, prediction of future outcomes. The main motivation behind building a model is to redress design debug and other shortcomings afore the construction of the real building starts. Coloured Petri Nets [23] (CP-nets or CPNs) is a graphical language for constructing models of systems and analyzing their properties. CP-nets are a modelling language combining the capabilities of Petri nets with the capabilities of a high-level programming language. An advantage to using CPNs is to use the same models to check both the logical or functional correctness of a system.

VII. LOCALIZATION

Due to unavailability of GPS signal underwater, WSN localization techniques can't be applied to UWSN. Underwater communication is based on acoustic waves. These localization methods are divided into two approaches: Range-based approaches and Range-free approaches [4].

a) Range-Based Localization Schemes

Time of Arrival (TOA), Time Difference of Arrival (TDOA) or Received Signal Strength Indicator (RSSI) is used for distance estimation. Some nodes which are known in advance by anchor are known its location to localize the other nodes in the network. By measuring the distance between anchor and the node, it can be specify the coordinates.

An Anchor Free Localization Algorithm (**AFLA**) is scheme, where no anchor nodes are deployed. Nodes are tied to anchor by cable to prevent it from its mobility. It is self-localization algorithm. It benefits from of adjacent nodes.

A Hierarchical Localization Approach (**LSL**) for large-scale 3D network is a distributed approach used that is based on 3D Euclidean distance estimation. It classifies nodes into three types: surface buoy, anchor node and normal node. GPS locate the surface buoy where it locates the anchor node which is responsible for ordinary nodes localization. It is simple and has low overhead communication.

A Time Synchronization Free Localization Scheme (**LSLS**) for large scale UWSN. Three surface buoys hear each other using TDOA measured at a sensor node. Reactive beaconing is used for time synchronization. A localized node becomes a reference node to the others iteratively to maximize coverage besides scheme to evaluate the variable sound speed.

Table 10: Comparison of UWSN simulation programs [21].

Simulator	Programming Language/Platform	Open Source and Online Documents	Limitations
NS-2	C++	Yes	Complicated, Time consuming GUI didn't support.
EmStar	Linux	Yes	Limited scalability, low reality, real time simulation accessed only.
GloMoSim	Parsec	Yes	Only wireless network, limited in IP network and routing protocols.
Shawn	Java	Yes	It doesn't care of low layer and restricted to postscript files.
UWSim	C++		Restricted number of functionalities, used only for UWSN.
VisualSense	Ptolemy II		Limited in protocols.
J-Sim	Java	Yes	Difficulty and latency.
OMNeT++	C++	Noncommercial License, Commercial License	Bug report Compatibility and probability.
Aqua-Sim	C++	Yes	An acoustic signal is very slow
QualNet	C++	Commercial License	

Underwater Sensor Positioning (**USP**). It changes the problem from 3D to 2D by employing sensor nodes' depth Bilateration and determineslocalizationof all nodes using iterative localization in 3D network with three surface buoys to help. It is based on find out the node location in 2D which helps to determine it in 3D planes.

Underwater Positioning System (**UPS**) scheme: it is silent scheme which no time synchronization is used. It is used four reference nodes with one deployed underwater for this purpose. TDOA from reference nodes is used to measure sensor nodes range. UPS reach out to Wide Coverage Positioning Scheme (**WPS)**which use five references to overcome infeasible region in UPS. But it is lowest Performance than UPS in spite of its high probability localization.

Dive and Rise (**DNR**): GPS locate its coordinate when it float to sea surface and after that sink down to a certain depth and backonce more. During this, sensor nodes listen passively to DNR massage and use three or more messages to localize itself. It uses TOA as a silentpositioning scheme for distance calculation.

Multistage localization using mobile beacon (PL). It solve the problem of low depth of DNR diving. Meandering Current Mobility (MCM) model is used to consider node mobility.

A Three Dimensional Underwater Localization **(3DUL)** Localization process is classified into two steps: 1. ranging and 2. Projection and dynamic trilateration. 1^{ST} phase, distance measurement between sensor nodes is done by estimated sound speed and two ways message and three neighboring anchor nodes. Three anchors are used in next phase to project to plane to localize nodes. Robustness of anchor helps trilateration to locate.

b) Range-Free Localization Schemes

It does not use TOA, TDOA, RSSI which it estimate the position of nodes.

An Area Localization Scheme (**ALS**): it estimates the certain location using acoustic signal from reference nodes with different power. For acoustic signal, the model of spherical propagation is used. the minimum power level received is recorded and send to a central server. This server uses its information to localize the node. Communication range, centralization and estimation of coordinate are the major limitations.

A localization scheme Using Directional Beacons (**UDB**). An AUV tour with directive antenna sending signals at some angle toward nodes Sensor nodes watch these signals to find outits position. It is an energy efficient technique because passive listen. Time synchronization is not used [4].

UDB is developed for 3D underwater network by Localization with Directional Beacon (**LDB**). LDB is a distributed approach which use for sparse and dense networks. An AUV use directive device while surfing over certain area in the network and sends directional beacons toward sensor nodes. The first and last herd beacons determine the node's coordinates. Use different depth to node is the basic difference from UDB and nodes are tied to sea ground to prevent them from moving. It is saving energy as silent scheme. Localization inaccuracy is upper bounded [4]. The comparison between schemes is mentioned in Table 11.

VII. FUTURE WORK

Based on current research work in UWSN routing protocols, it is clear that many issues are unsolved. Some of these issues listed as follows:

- The routing must be self-configuring because in case of failure; equipment is deployed far from the experts.
- Implementing the existing routing protocols with security mechanisms involvement.
- Design routing protocols that handle multi-copy mechanism, when one copy of the packet reached the destination, then how the intermediate nodes know to discard the other copies of the same packet, for the best use of the resources.
- Most existing void handling techniques in UWSNs employ flooding techniques to find the turn link, proposing new void handling methods with low overhead.
- Design an efficient routing protocol that balance between the nodes energy and the communication overhead.
- Design a new technique which converts different energy types such as moving energy to electrical energy
- In location-based routing protocols, it is necessary to devise efficient underwater location discovery techniques.
- In location-based routing protocols, since each transmitted data packet contain location information, it is necessary to focus on the node location privacy.

In general, the various research issues facing UWSN researchers are in the following aspects: network topology, physical layer, MAC layer, Network layer, and Application layer. Reference [5] stated the problems related the network layer as follows:-

TABLE 11: Comparison of localization schemes [4].

Scheme	Range based/Range free	Range Measurement Using	Time Synchronization Required	Silent Positioning	Node Mobility Considered	Iterative Localization Used
DNR	range based	TOA	Yes	Yes	Yes	No
PL	range based	TOA	Yes	Yes	Yes	Yes
LSL	range based	TOA	Yes	Yes	Yes	Yes
AFLA	range based	TOA	Yes	No	Yes	No
LSLS	range based	TDOA	No	Yes	No	Yes
USP	range based	TOA		Yes	No	Yes
3DUL	range based	Two way message exchange	No	No	Yes	Yes
UPS	range based	TDOA	No	Yes	No	No
WPS	range based	TDOA	No	Yes	No	No
UDB	range free	N/A	No	Yes	No	No
LDB	range free	N/A	No	Yes	No	No
ALS	range free	N/A	No	Yes	No	No

- Connectivity loss management without provoking immediate transmissions, delay-tolerant applications have to be developed for.
- Healthy routing algorithms is required, Due to the quality of acoustic links is highly unpredictable, with respect to intermittent connectivity of acoustic channels.
- Connection failure must be addressed through protocols besides, mobility of nodes and battery depletion.
- Development of underwater location discovery efficiently in geographical routing protocols.
- Development of simulation models and tools to understand data transmission's dynamics.

The propagation delay depends on the distance betweenthe nodes and it is larger in horizontal acoustic links than vertical one because of multipath.

VIII. CONCLUSIONS

Interest in UWSNs is increasing, and related research studies are in progress. However, underwater environment is a special environment that has many restrictions. Considering this restriction, many challenges face the design of the routing protocols of UWSNs. The routing protocols in UWSNs have the common objective of trying to increase the delivery ratio while decreasing the resource consumption and End-to-End delay. However, current routing protocols have not designed to defend against security attacks that can block or degrade network communication and performance.

In this paper, we introduced an overview of UWSNs its characteristic, challenge, communication system nature, network architecture, localization and applications. We discuss some of UWSNs routing protocols and study their advantages and disadvantages. The comparison is necessary in order to point out which routing protocol is best according to the desirable use. We also explored security issues and attacks of UWSNs. We present comparison between the surveyed routing protocols according to its vulnerability against various security attacks. Security issues in UWSNs remain open and we expect to see more research activities on these topics in the future.

REFERENCES

[1] Dina M. Ibrahim, Mohmoud M. Fahmy, Tarek E. ElTobely, and ElSayed A. Sallam, "Modelling and Performance Enhancement of Underwater Wireless Sensor Networks by Petri Nets", Thesis submitted to the Engineering Faculty, Tanta University, for the degree of Doctor of Philosophy in Electrical Engineering, 2014.

[2] Jian S., Jin W., Jianwei Z. and Shunfeng W., "A Comparative Study on Routing Protocols in Underwater Sensor Networks", Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Lecture Notes in Electrical Engineering 260, Springer Science & Business Media Dordrecht, 2014.

[3] M.Kiranmayi1and Dr. Kathirvel Ayyaswamy; 'Underwater Wireless Sensor Networks: Applications, Challenges and Design Issues of the Network Layer - A Review', International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.1, January 27, 2015, pp. 05 – 11.

[4] Mukesh Beniwal and Rishipal Singh, 'Localization Techniques and Their Challenges in Underwater Wireless Sensor Networks', International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4706-4710.

[5] Bhanu K., "Muti-Metric Adaptive Routing Algorithm for Underwater Wireless Sensor Networks", a thesis submitted in partial fulfillment of the requirements for the Degree of master of

science, Texas A&M University - Corpus Christi Corpus Christi, Texas, 2011.

[6] Ahmed M., “Iraqi Rivers Pollution Monitoring System Based on Underwater Wireless Sensor Networks”, a thesis submitted to the Computer Engineering Department University of Technology in Partial Fulfillment of the requirements for the Degree of Master of Science in computer engineering, 2013.

[7] Salvador Climent, Juan Vicente Capella, Nirvana Meratnia and Juan José Serrano, ‘Underwater Sensor Networks: A New Energy Efficient and Robust Architecture’, Sensors 2012, 12, pp.704-731.

[8] MohsinMurad, Adil A. Sheikh, Muhammad AsifManzoor, EmadFelemban, and SaadQaisar, ‘A Survey on Current Underwater Acoustic Sensor Network Applications’, International Journal of Computer Theory and Engineering, Vol. 7, No. 1, February 2015, pp.51-56.

[9] Parul Garg and Sandeep Waraich, ‘ Parametric Comparative Analysis of Underwater Wireless Sensor Networks Routing Protocols’, International Journal of Computer Applications, Vol.116 No. 11, April 2015, pp. 29-35.

[10] Sihem Souiki, Maghnia Feham, Mohamed Feham and Nabila Labraoui, ‘Geographic Routing Protocols for Underwater Wireless Sensor Networks: A Survey’International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 1, February 2014, pp.69-87.

[11] Kifayat Ullah Jan and Zahoor Jan, ‘Survey on Routing Protocols for Under Water Sensor Networks’, Journal of Computer Engineering (IOSR-JCE), Vol. 16, Issue 1, Ver. VI, Feb. 2014, pp. 44-46.

[12] Xie P., Cui J., and Lao L, “Vector-based Forwarding Protocol for Underwater Sensor Networks”, International conference on networking (IFIP networking), 2006.

[13] Nicolaou N., See A., Xie P., Cui J., and Maggiorini D., “Improving the Robustness of Location-based Routing for Underwater Sensor Networks”, Proc. Of the OCEANS’07, Europe, IEEE, 2007.

[14] Xie P., Zhou Z., Peng Z., Cui J.-H., and Shi Z , “Void Avoidance in Three-dimensional Mobile Underwater Sensor Networks”, Proc. of the 4th international conference of wireless algorithms, system, and applications (WASA), USA, 2009.

[15] Bo W., Yong-mei L, and Zhigang J, “ES-VBF: An Energy Saving Routing Protoco”, In Proceedings of the International Conference on Information Technology and Software Engineering, 2012.

[16] Dina M. Ibrahim, Mohmoud M. Fahmy, Tarek E. ElTobely, and ElSayed A. Sallam, “Enhancing the Vector-Based Forwarding Routing Protocol for Underwater Wireless Sensor Networks: A Clustering Approach”, The Tenth International Conference on Wireless and Mobile Communications (ICWMC), 2014.

[17] Yonca B., Nirvana M. and Aylin K., “A Comparative View of Routing Protocols for Underwater Wireless Sensor Networks”, Proc. of the OCEANS’11, Spain, IEEE, 2011.

[18] Mari C.,” Securing Underwater Wireless Communication Networks”, IEEE Wireless Communications, 2011.

[19] Muhammad Ayaz, Imran Baig, Azween Abdullah and Ibrahima Faye, ‘A survey on routing techniques in underwater wireless sensor networks’, Journal of Network and Computer Applications, 2011, pp. 1-20.

[20] Thumpi.R, Manjula R.B and SunilkumarS.Manvi, ‘A Survey on Routing Protocols for Underwater Acoustic Sensor Networks’, International Journal of Recent Technology and Engineering (IJRTE), Vol.2, Issue.2, May 2013, pp. 170-175.

[21] V.P. Dhviya, R. Arthi, “Analysis of Simulation Tools for Underwater Wireless Sensor Networks”, International Journal of Computer Science & Engineering Technology (IJCSET), 2014.

[22] P. Xie, Z. Zhou , Z. Peng , H. Yan , T. Hu , J. Cui , Z. Shi , Y. Fei& S. Zhou “Aqua-Sim: An NS-2 Based Simulator for Underwater Sensor Networks”, in proc. Of MITS/IEEE oceans conference, 2009.

[23] K. Jensen, L. Kristensen and L. Wells, “Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems”, International Journal on Software Tools for Technology Transfer (STTT), Springer-Verlage, 2007.

Prof. S. El-Rabaie (SM’92) was born in Sires Elian, Egypt, in 1953. He received the B.Sc. degree (with honors) in radio communications from Tanta University, Tanta, Egypt, in 1976, the M.Sc. degree in communication systems from Menoufia University, Menouf, Egypt, in 1981, and the Ph.D. degree in microwave Device engineering from Queen’s University of Belfast, Belfast, U.K., in 1986. In his doctoral research, he constructed a Computer-Aided Design (CAD) package used in nonlinear circuit simulations based on the harmonic balance techniques .Up to February 1989, he was a Postdoctoral Fellow with the Department of Electronic Engineering, Queen’s University of Belfast. He was invited as a Re-search Fellow in the College of Engineering and Technology, Northern Arizona University, Flagstaff, in 1992 and as a Visiting Professor at Ecole Polytechnique de Montreal, Montreal, QC, Canada, in 1994. He Has Authored and Co-authored of More Than 220 Papers and Eighteen text Books. He was Awarded several Awards (Salah Amer Award of Electronics in 1993, The Best Researcher on (CAD) from Menoufia University in 1995). He acts as a reviewer and member of the editorial board for several scientific journals. He Has Shared in Translating the First Part of the Arabic Encyclopedia. Professor EL-Rabaie was the Head of the Electronic and Communication Engineering Dept., Faculty of Electronic Engineering, Menoufia University, then the Vice Dean of Postgraduate Studies and Research in the same Faculty. Prof. S. El-Rabaie is Involved now in Different Research Areas including CAD of Nonlinear Microwave Circuits, Nanotechnology, Digital Communication Systems, and Digital Image Processing. Now he is Member of the National Electronic and Communication Eng. Promotion Committee and Reviewer of Quality Assurance and Accreditation of Egyptian Higher Education. e-mail;- srabie1@yahoo.com , Mobile:- 0128498170

Mohammed A. Alsharqawy was born in September 1984 in KSA. He graduated from faculty of engineering Tanta University in 2007 and received the MSc in 2014 from faculty of engineering Tanta University. It is about Cloud Computing and its application to serve for ERTU's cloud and its needs. He joined ERTU in 2008 and specialized in Transmission broadcast for TV. He concern about Digital communication, new trends, TV and Network.