ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.1, Pages : 05 – 11 (2015)
Special Issue of ICEEMC 2015 - Held during January 27, 2015, Chennai, India

Underwater Wireless Sensor Networks: Applications, Challenges and Design Issues of the Network Layer - A Review

M.Kiranmayi[1], Dr. Kathirvel Ayyaswamy[2]
[1]Research Scholar, India, sarathbabu.kiranmayi64@gmail.com
[2]Anna University, India,ayyakathir@gmail.com

Abstract*:* Underwater wireless sensor networks (UWSNs) consists of variable number of sensor and vehicles that are deployed to perform concert monitoring tasks over a specified area in the ocean. To achieve this, sensors and vehicles self-standardized in an autonomous network which can adapt the features of the oceanographic environment. Due to the peculiar characteristics of the underwater environment, some anti characteristics will seriously interfere with reliable data communication, information transmission rates, communication range, throughput and packet routing information of underwater sensor networks and also vulnerable to attacks due to the high bit error rates, Large propagation delays and low or insufficient bandwidth of acoustic medium. Underwater Sensor Networks and their ground information counterparts require the development of efficient algorithms, reliable security mechanisms and the entire involvement of node routing information while maintaining a correct and effective transmission of data, which increases the network lifecycle are essential when routing protocols for Underwater Sensor Networks. This paper explores the significant advantages, disadvantages of design issues of different routing protocols. UWSNs suffer from the vulnerabilities which decreases the reliability of a data and the network. So, this article also have discussed for security in UWSNs, underlying the specific characteristics of these networks, possible underwater attacks, their countermeasures and challenges.

Key words: UWSNs Design Challenges, Network Layer Issues and Routing Protocols, Underwater Wireless Security, Attacks and Countermeasures.

INTRODUCTION

Underwater Sensor Networks are a new genetic approach of networks which drives much attention in research developers. Today our earth is overlay by 75 percent of water either by rivers or by oceans where a large amount of data and resources lies and are needed to discover these hidden information, from the bottom of the underwater seashore surface. These underwater networks are widely utilized in research areas of aquatic applications to investigate the unexplored underwater surface. Some of the Underwater aquatic applications are (i) *pollution monitoring* such as oil-leakage in lakes or rivers, Chemical pollutions, Nuclear Pollutions in the environment, (ii) *Surveillance* in UAN has more accurate and low signatures can be achieved by using different sensors, (iii) *Mine Reconnaissance or Mine Detection* can detect mine like objects efficiently with the help of acoustic sensors and optical sensors, (iv) *Disaster Prevention* is used to monitor seismic activity such as Ocean- related disaster, undersea activities etc., can be informed to coastal areas when happen in real time, (v) *Assisted Navigation* is used to locate and identify various underwater threats like Rocks, Submerged Vehicles, Shoals etc [1, 14]. The fastest way of finding information which is available in Underwater Sensor network. This information is not only helpful for human beings but also responsible for researchers [14].

Basically communication in underwater environment is different from terrestrial networks due to its unique features of the networks. Underwater Networks are established by using acoustic signals as communication medium with the help of sensors and autonomous underwater vehicles. Since wireless sensor networks as in behavior of terrestrial networks, some different fundamental challenges are not suitable for underwater usage, such as (i) *Radio Signals* transmits long distances at extra low frequencies, which requires large antennas and high transmission power [1] and (ii) Due to the continuous movement of sensor nodes with water flow, Global Positioning System (GPS) is inapplicable to the underwater environment [2]. Hence Underwater Wireless Networks are depends on the Acoustic Communication medium. Therefore the major issue in these networks is that how the sensing data are routed and successfully delivered to the sinks.

A large number of routing protocols have been proposed for finding a path from source node to sink in the Terrestrial Wireless Sensor Networks [3, 4]. However these protocols are designed based on an end-to-end method that is not applicable to high dynamic topology networks with high propagation delay (e.g., UWSNs) [5, 6]. Since UWSNs is a very recent issue in this area of study, most researchers focus on Physical Layer [7, 8], Data Link Layer [9, 10], and localization [11, 12], whereas research on network layer is still in its infancy stage.

Thus research programmers are being undertaken for designing efficient protocols considering the unique characteristics of the Underwater Communication Networks.

CHALLENGES IN UNDERWATER WIRELESS SENSOR NETWORKS

In this section, we discuss about challenging issues of the Underwater Networks, and then proceed to communications and networking layers, followed by a discussion on various security issues of network layer.

Topology: High dynamic due to the continual movement of sensor nodes by the current movement of the water.

Communication Media: Acoustic waves for underwater environment and radio waves for water surface.

Position information: Unavailable by GPS, because GPS uses high frequency waves which are rapidly absorbed in the sea water.

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

Range: Usually used in vast ocean areas.

Speed of Medium: Acoustic Velocity in water is about 1500 m/s.

Price: Too expensive.

Path Loss: High path loss.

Wave movement: Spherical in deep water and Cylindrical in shallow water.

Sink Position: Located on water surface and it usually moves by water current.

Routing: Due to high movement of nodes in water current, greedy hop-by-hop routing is employed.

Prone to error: Links and nodes are highly prone to error due to high propagation delay of acoustic waves and corrosion respectively.

Sensors Size: Large size.

RESEARCH ISSUES IN UWSN

The various research issues facing UWSN researchers in the following aspects: network topology, physical layer, MAC layer, Network layer, and Application layer. Here we have discussed only related to network layer.

NETWORK TOPOLOGY

Due to the uniqueness of underwater channels and characteristics of acoustic signal, UWSN network topology is different from ground-based counter parts. However, the fundamental design goals are the same, i.e., providing reliable connectivity among nodes in the network; increasing network capacity; and minimize the energy consumption.

Basically, two types of network topologies can be used: ad hoc mode and hierarchy mode. In the ad hoc mode, nodes are self-organized as a P2P network, as shown in Fig 1.

Peer-to-peer topology can be further divided into point-to-point connection topology, and multi-hop connection one. There is just one hop from a node to any other node in the first type of connection, i.e., routing is not necessary. In the latter one, other nodes are involved to relay a data message from a source node to its destination. In other words, routing is needed with this second type of network topology. It is found that multi-hop topology is more energy efficiency [15] [16] in ground based wireless networks. This conclusion needs to be investigated and extended to UWSNs.

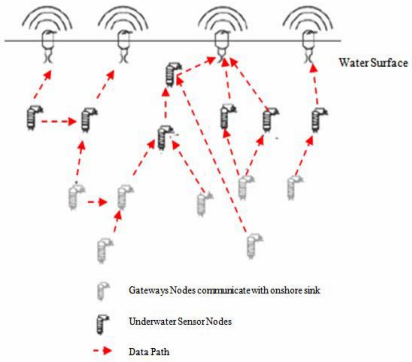

Fig 1: Ad Hoc Mode

The Fig 2 shows an example of hierarchy network topology in which several levels of the structure are deployed. Depending on the ways to place nodes (e.g., permanent or on-demand deployment), the time constraints imposed by the applications, and the amount of data being retrieved, various kinds of topologies can be applied to a UWSNs.

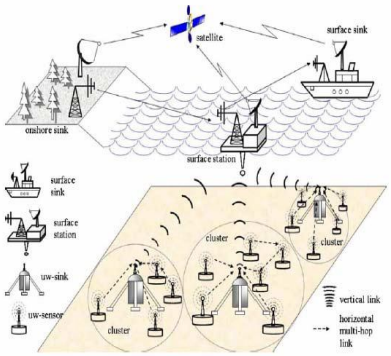

Fig 2: Hierarchy Mode

NETWORK LAYER

If the network range is not large and one hop is sufficient to deliver information, then there is no need for relaying message. Otherwise, when it increases such that single-hop transmission is insufficient, multi-hop is needed to relay information from source to destination. It is also shown that multi-hop delivery is more energy efficiency in underwater network than single-hop delivery does [17]. The network layer determines the path from a source node to the destination one when multi-hop is needed.

Basically, there are two methods of routing. The first one is virtual circuit routing and the second one is packet-switch routing. In virtual circuit routing, networks use virtual circuits to decide the path at the beginning of the network operation. In packet-switch routing, each and every node that is part of the transmission makes its own routing decision, i.e., decides its next hop to relay packet. Packet-switch routing can be classified into proactive routing and reactive routing protocols. Most routing protocols for ground-based wireless networks are packet-switch based.

Proactive routing protocols attempt to minimize the message latency by maintaining up-to-date routing information at all times from each node to any other node. It broadcasts the packets that contain routing table information to all the nodes. Typical protocols include Destination sequence Distance Vector (DSDV) [18] and Temporally Ordered Routing Algorithm (TORA) [19]. However, proactive routing protocols provoke a large signaling overhead to establish routes for the first time and each time the network topology changes. It may not be a good fit in underwater environment due to the high probability of link failure and extremely limited bandwidth there. In contrast, reactive routing protocols only initiate a route discovery process upon request. Correspondently, each node does not need to maintain a sizable “look-up” table for routing. This kind of routing protocols is more suitable for dynamic environment like ad hoc wireless networks [20, 21]. Typical protocol examples are Ad hoc On-demand Distance Vector (AODV) [22], and Dynamic Source Routing (DSR) [23].

The shortage of reactive routing protocols is its high latency to establish routing. Similar to its proactive counterpart, flooding of control packets to establish paths is needed, which brings significant signal overhead. The high latency could become much deteriorated in underwater environment because of the much slower propagation speed of acoustic signal compared with the radio wave in the air.

When compared to the above routing protocols, Virtual-circuit switch routing protocols can be a better routing protocol for underwater acoustic networks. The justifications are:

1. Underwater acoustic networks are typical asymmetric instead of symmetric. However, packet switched routing are proposed for symmetric network architecture;
2. Virtual-circuit switch routing protocols work for robust against link failure, which is crucial in underwater environment;
3. Virtual-circuit switch routing protocols have less signal overhead and low latency. These factors are necessary for underwater acoustic channel environment.

However, virtual-circuit switch routing protocols usually lack of flexibility. How to focus the degree of flexibility into virtual-circuit-switch routing protocols is a question that needs to be answered by UWSN network layer research.

The main objective of the network layer is to allow end system, connected to different networks, to exchange data through intermediate systems called router. It finds the path from source to the destination while taking into consideration of the characteristics of the channel.

RESEARCH ISSUES IN NETWORK LAYER

1. To manage loss of connectivity without provoking immediate transmissions, mechanisms have to be developed for delay-tolerant applications.
2. Due to fading and multipath, the quality of acoustic links is highly unpredictable, with respect to intermittent connectivity of acoustic channels, healthy routing algorithms is required.
3. Protocols and algorithms are required to be developed to address connection failures, unforeseen mobility of nodes and battery depletion.
4. In case of geographical routing protocols development of efficient underwater location discovery techniques are to be developed [24].
5. To understand dynamics of data transmission at the network layers, credible simulation models and tools are required to be developed for accurate modeling.
6. The delay variance of acoustic signals to propagate from one node to another heavily depends on the distance between two nodes. The delay variation in horizontal acoustic links is generally larger than in vertical links which is due to multipath [25].

ROUTING PROTOCOLS FOR UWSN

Routing is one of the major fundamental issues in the network. However, researchers have less attention about the layer called network layer or routing layer, and research in this routing layer is still in its infancy [26]. Since the main objective of the network layer is routing [37, 38], designing efficient and practical routing protocols for underwater environment that consider the underwater challenges are essential.

According to the requirements of different applications in underwater wireless environment, researchers have proposed different routing protocols to improve the various performance metrics in the network layer [26]. As previously mentioned, due to characteristics of acoustic channel and underwater environments, end-to-end routing methods applied for Terrestrial Wireless sensor Networks (TWSNs) are inapplicable in the Underwater Wireless Sensor Networks (UWSNs).

According to the literature, due to high mobility of nodes with water flow movement, greedy hop-by-hop routing is the most suitable routing technique for UWSNs. This technique rest on a particular simple forwarding strategy at every hop, a data packet has to transmit to a local optimal forwarder node with a positive progress towards the sink node.

In the greedy hop-by-hop routing technique, communication void is one of critical problems in which routing approaches should be able to handle. For any Greedy routing protocol, handling the communication void problem is a technical challenge [27]. In general, greedy routing protocols are composed of two methods, namely, greedy method and void handling method [27, 29]. The greedy mode works only when each node has at least one neighboring nodes with positive progress towards the sink; otherwise, it changes the mode to void handling mode due to the communication void problem.

In order to forward the data packets in the greedy mode, each node sends the data packet to a set of neighbor nodes with positive progress toward the sink. As a result, with the greedy mode, finding a set of neighbor nodes with positive progression, toward the sink is a crucial factor. Since the sinks in UWSNs are deployed in the water surface and ordinary nodes are scattered in the different depths of the underwater network, neighbor nodes with positive progress towards the sink are located in the top of the forwarding node. Otherwise, the neighbor nodes with positive progress have less depth than the current forwarding node. As stated by this information, greedy routing can be utilized easily in UWSNs.

Due to the unique challenges of underwater environment, the protocols proposed for terrestrial networks cannot be directly applied to UWSNs. Many routing protocols have been proposed for UWSNs taking into consideration, the unique features of underwater networks, including medium access control, network protocols and transport protocols. The routing protocols for UWSNs can be classified into localization-based and localization-free routing protocols . These protocols are greedy routing protocols and can take advantage of the localization of sensor nodes; however, the localization is imperfect due to the mobility of sensor nodes in the network, and harsh environment. Otherwise localization-free routing protocols are highly demanded by researchers.

Recently, many routing protocols have been proposed for UWSNs. In this paper, we present some important known routing protocols proposed for UWSNs, which can be classified into two sections, localization-based and localization-free routing protocols.

ROUTING PROTOCOLS

These routing protocols are geographic routing protocols and are used to locate its position in the network based on the assumption of the localization of sensor nodes.

VBF

Vector Based Forwarding (VBF), mechanism was proposed in the paper [30]. VBF is a path based forwarding protocol. It represents a path with a “routing vector” from the source to the sink. Intuitively a virtual pipe with the source-to-sink vector as the axis is used as the abstract route for data delivery. If the pipe is “populated” by nodes then the data packets can be forwarded to the sink. The radius of the virtual pipe is a predefined distance threshold. For any sensor node which receives data, it first computes its distance to the routing vector. If this distance is smaller than the threshold, then the node is considered as a candidate to forward the data.

Otherwise, the node simply discards the data. To reduce the traffic in dense networks, VBF adopts a distributed self-adaptation algorithm, in which all the candidate nodes are coordinated and finally only several most “desirable” ones can forward the data packets. VBF can significantly reduce network traffic, thus saving energy. It is also robust to topology dynamics since it is a location-based on-demand routing protocol, and no pre- computed routes maintained in sensor nodes. There are two major drawbacks with VBF:

1. Because of the use of the unique source-to-sink vector, the creation of a single virtual pipe may significantly affect the routing efficiency in different node density areas.
2. Again because of the single source-to-sink vector design, VBF is too sensitive to the routing pipe radius threshold.

HH-VBF

To overcome the above problems in HH-VBF, protocol. Hop-by-Hop Vector-Based Forwarding (HH-VBF) [31] is uses the same concept of routing vector as VBF. However, instead of using a single virtual pipe from the source to the sink, HH-VBF defines a different virtual pipe around the per-hop vector from each forwarder to the sink. In this way, each node can adaptively make packet forwarding decisions based on its current location.

The advantage is, HH-VB can find delivery path even if the number of nodes available in the forwarding path is very limited in number. It has good packet delivery ratio and more signaling overhead than VBF. Simultaneously it faces the routing pipe radius threshold problem, which affecting the performance.

FBR

Focused Beam Routing [32] is a scalable routing technique based on location information. The focused beam routing protocol works on the geographical routing. It is presented as a suitable routing protocol for both mobile and static underwater sensor networks without the need of the clock synchronization. In FBR every node in the network is expected to be aware of its location and every source node should be aware of its destination.

The advantage of FBR is to restrain the flooding by the transmission power, so that energy consumption is reduced. Simultaneously it faces the problems due to water movements, nodes does not lie in the forwarding cone of angle. If some nodes are positioned outside the forwarding area, it is forced to retransmit the RTS eventually resulting in the increase in communication overhead.

DFR

DFR (directional flooding based routing) protocol [33] employs scoped flooding for the transmission of the data packets. The packets are transmitted in a restricted flooding zone where the zone area is selected based on an angle formed by the vectors. It enhances reliability by packet flooding technique. The assumption is the geographic information is available to all the nodes i.e. the location information of the neighboring nodes and the destination node. Link quality is the foundation for deciding the forwarding nodes. Good quality links limit the number of nodes in the flooding zone. Void problem is rectified by the selection of at least one node to transmit the data packet towards the sink. Simultaneously reverse transmission of data packet is impossible, if the sending node cannot find a next hop closer to the sink. In such a situation void problem cannot be rectified.

REBAR

REBAR (Reliable and Energy Balanced Routing Algorithm) is a location based routing protocol. Geographic information is used by the nodes between the source and the sink to transfer the data. The packet is assigned with a unique identifier (ID), which is composed of the source ID and a sequence number. The packet is broadcasted in the network. Each receiver maintains a buffer to record the ID of recently received packets. Duplicates can be treated by the history and will be discarded. REBAR uses an extended mechanism to bypass routing voids in the network by the assumption that the nodes on the boundary of the voids can detect the existence of voids using the methods [34] [35].

The nodes in the network can be divided in to two different sets: Boundary set and Non-Boundary set. When a node in the Non-Boundary-Set receives a packet, it behaves as in the basic REBAR. While a node in the Boundary-Set, forwards the packet to all their neighbors directly without checking distance and vector information.

SBR-DLP

A sector-based routing with destination location prediction (SBR-DLP) have introduced in [36]. In this routing, a node knows its own location, and the location of the predicted destination node. Consequently, it relaxes the need for accurate knowledge of the destination's location. In SBR-DLP the sensor nodes are not required to carry neighbor information or network topology. Each node is assumed to know its own position, and the destination node's pre-planned movements. This movement is usually predefined prior to launching the network. A hop-by-hop fashion is used to route the packet to the destination, instead of finding the complete path before sending a packet.

The limitation of this concept is that, post launch position changes are impossible. Moreover scheduled movements of destination nodes can be affected by underwater currents.

The SBR-DLP allows the sender determine its next hop using information received from the candidate nodes. Thus proposed SBR-DLP is different from both VBF and HH-VBF; which let each candidate node decide whether it should relay the packet; this eliminates the problem of having multiple nodes acts as a relay nodes, which is experienced in both VBF and HH-VBF.

LCAD

LCAD (Location Based Clustering Algorithm for Data Gathering) is a clustering algorithm. The protocols used in terrestrial networks such as LEACH, HEED, cannot be directly applied to underwater sensor networks due to the nature of the aqueous medium. The underwater networks uses the acoustic waves and hence the propagation delay incurred in an underwater sensor network is higher than its terrestrial counterpart. Moreover the sensors are deployed in a three dimensional topology, which can address the problem of rapid energy drains of sensor nodes around the sink. The sensor nodes are fixed relative depths. Sensor nodes in each tier are deployed in clusters with multiple cluster heads. According to the node position, this algorithm selects cluster head at each cluster. Data packet collection from the cluster heads are done by AUVs. LCAD uses two-level addressing scheme within the network, the first is used for intra cluster communication, and the second for inter cluster communication.

LCAD performance depends on the position of cluster head inside the grid structure. This structure is less applicable for UWASN due to the non consideration of node movement in the network.

UNDERWATER WIRELESS SECURITY

The attacks against geographic routing in UWSNs are the same as in terrestrial sensor networks. The same countermeasures cannot be directly applied to UWSNs due to their difference in characteristics such as: the large propagation delays, the low bandwidth, the difficulty of recharging batteries of underwater wireless sensors, and the high mobility of nodes in underwater environment.

Data Confidentiality

Confidentiality is an assurance of authorized access to information. It is the ability of the network to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. Thus, it ensures the protection of sensitive information and not revealed to unauthorized third parties. Applications like maritime surveillance communicate highly sensitive data.

Data Integrity

Data integrity is to ensure that information is not modified in transit, either due to malicious intent by an attacker. Thus, integrity is an assurance that packets are not modified in transmission.

Data Authentication

Data authenticity is an assurance of the identities of communicating nodes. WSN communicates sensitive data to help in many important decisions making. Thus, it is very important for every node to know that a received packet comes from a real sender. Otherwise, the receiving node can be cheated into performing some wrong actions. Also, authentication is necessary during exchange of control information in the network.

Data Freshness

Packet replaying is a major threat to the freshness requirement in network communication, so as to prevent a packet from continuing to a destination, and hold it for any amount of time, and then reply it into the network. The obsolete information available in the packet can cause many problems to the applications deployed in the network.

Availability

Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may block the communication to make sensors unavailable. The requirement of security not only affects the operation of the network, but also important in maintaining the availability of the network node should not break the security of the entire network.

Self Organization

UWSN is typically an ad hoc network, in which every sensor node in the network be independent and flexible enough to be self-organizing and self-healing according to different conditions and no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature also brings a big challenge to underwater wireless sensor network security.

Secure localization

The use of an underwater wireless sensor network will depend on its ability to accurately and automatically locate each node in the network. This accurate location information is needed inorder to identify the location of a fault in the network.

Robustness and Survivability

The sensor network should be robust against various security attacks, and if an attack targets, then its impact should be minimized.

ATTACKS AND COUNTERMEASURES

In computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Jamming attack

It is a type of attack which interfere physical channel that the nodes use in a UWSN for communication by putting noises or meaningless signals. A jamming source may be powerful enough to disrupt the entire network. A jamming attack consists of interpose with the physical channel by putting up carriers on the frequencies neighbor nodes use to communicate. When an attacker intendly jammed the communication between a sender and a receiver, and later replays the same message with stale information posing as the sender.

Counter measures

It can be overcome using following two techniques are:

1. Spread spectrum techniques
2. Sensors can switch to sleep mode.

Wormhole Attack

A wormhole is an out-of-band connection created by the antagonist between two physical locations in a network with lower delay and higher bandwidth than ordinary connections. In a wormhole attack the malicious node transfers some selected packets received at one end of the wormhole to the other end using the out-of-band connection, and refill them into the network.

Counter measures

It can be overcome using following two techniques are:

1. Dis- VoW
2. Estimating the direction of arrival.

Sinkhole Attack

In a sinkhole attack, a malicious node attempts to provide a false routing information to other nodes, and produce itself as the intented node to receive the entire network traffic and modifies the secret information available in the packet. For example, the malicious node can produce a better route, by that exchange of routing take place. The *sinkhole* attack is a particularly violent attack that prevents the base station from obtaining complete and accurate sensing data, thus forming a serious threat to other layers in the network. Geographic routing and authentication of nodes exchanging routing information are possible countermeasures against this attack, but even geographic routing in UWSN is a challenging open research topic.

Counter measures

It can be overcome using following two techniques are:

1. Geographical routing
2. Authentication of nodes exchanging routing information.

Sybil attack

In this an attacker with multiple identities can pretend to be in many places at once. Multiple identities can be occupied within the sensor network either by fabricating or stealing the identities of authorized nodes. Effectiveness of fault-tolerant schemes can be reduced by this attack. Sybil attacks also pose a high threat to geographic routing protocols. Authentication and position verification are methods against this attack, while position verification in UWSNs is difficult owing to mobility.

Counter measures

It can be overcome using following two techniques are:

1. Authentication
2. Position verification

Selective forwarding attack

Malicious nodes drop certain messages instead of forwarding them to delay routing. In UWSNs it should be verified that a receiver is not getting the information due to this attack and not because it is located in a shadow zone. Selective forwarding attacks may corrupt some mission critical applications such as military surveillance and Environmental monitoring

Counter measures

It can be overcome using following two techniques are:

1. Multipath routing
2. Authentication.

Hello Flood Attack

A node receiving a hello packet from a malicious node may interpret the false assumption about the attacker is a neighbor and the node will assume that the neighbor node is inside the radio range and forward all 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 link verification method can protect against this attack, although it is not accurate due to mobility of the nodes and the high propagation delays of UWSNs. Authentication is also a possible defense.

Counter measures

It can be overcome using following two techniques are:

1. Bidirectional link verification
2. Authentication in a possible defense.

Acknowledgment Spoofing

A malicious node overhearing packets sent to its neighbor nodes can use this information to deceive link layer acknowledgments with the objective of reinforcing a weak link which is located 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.

CONCLUSION

While research on underwater wireless sensor networks has significantly advanced in recent years, it is clear that a number of challenges still remain to be solved. With the flurry of new approaches to communication, medium access, networking and applications, effective analysis, integration and testing of these ideas is paramount—the field must develop fundamental insights, as well as understand what stands up in practice. This paper explores the significant advantages, disadvantages of design issues of different routing protocols. UWSNs suffer from the vulnerabilities which decreases the reliability. So, this article also have discussed for security in UWSNs, underlining the specific characteristics of these networks, possible attacks, countermeasures and challenges.

REFERENCES

[1]. M. Stojanovic, "Acoustic (underwater) communications," in *Encyclopedia of Telecommunications*, J. G. Proakis, Ed. John Wiley and Sons, 2003.

[2]. P. Xie, J.-H. Cui, and L. Lao, "VBF: vector-based forwarding protocol for underwater sensor networks," *Networking*, vol. 3976, pp. 1216–1221, 2006.

[3]. F. Akyildiz, W. Su, Y. ankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[4]. J.N. Al-Karaki and A. E. Kamal , "Routing techniques in wireless sensor networks: a survey," *IEEEWireless Communications*, vol.11, no. 6, pp. 6–27, 2004.

[5]. I. F. Akyildiz, D. Pompili, and T. Melodia, "State-of-the-art in protocol research for underwater acoustic sensor networks," in *Proceedings of the 1st ACM International Workshop on Underwater Networks*, pp. 7–16, September 2006.

[6]. I. F. Akyildiz, D. Pompili, and T.Melodia, "Challenges for efficient communication in underwater acoustic sensor networks,"

[7]. *ACM Sigbed Review*, vol. 1, pp. 3–8, 2004.

[8]. J. M. Hovem, "Underwater acoustics: propagation, devices and systems," *Journal of Electroceramics*, vol. 19, no. 4, pp. 339–347,2007.

[9]. J.-H. Jeon, T.-H.Won, H. Cho, and S.-J. Park, "Implementation of a micro-modem for underwater wireless sensor networks," in *Proceedings of the OCEANS IEEE-Spain*, June 2011.

[10]. H. T. Nguyen, S. Y. Shin, and S. H. Park, "State-of-the-art in MAC protocols for underwater acoustics sensor networks," in *Proceedings of theconference on Emerging direction in embedded and ubiquitous computing*,, vol. 4809, pp. 482–493, 2007.

[11]. N. Chirdchoo,W.-S. Soh, and K. C. Chua, "Aloha-based MAC protocols with collision avoidance for underwater acoustic networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications*, vol. 1–5, pp. 2271–2275, May 2007.

[12]. Z. Zhou, J. H. Cui, and S. L. Zhou, Localization for large-scale underwater sensor networks," in *Proceedings of the 6th international IFIP-TC6 conference on Ad Hoc and sensor networks,wireless networks, next generation internet*, vol. 4479, pp. 108– 119, 2007.

[13]. A. Y. Teymorian, W. Cheng, L. Ma, X. Cheng, X. Lu, and Z. Lu, "3D underwater sensor network localization," *IEEE Transactions on Mobile Computing*, vol. 8, no. 12, pp. 1610–1621, 2009.

[14].Yonca Bayrakdar, Nirvana Meratnia, Aylin Kantarci,A comparative view of routing protocols for underwater wireless sensornetworks.978-1-61284-4577 00880/11/$26.00,2011IEEE.

[15]. Ian F. Akyildiz, Dario Pompili, Tommaso Melodia, State of the Art in Protocol Research for Underwater Acoustic Sensor Networks, WUWNet06, September 25, 2006, Los Angeles, California, USA, ACM 1-59593-484-7/06/0009...$5.00.

[16]. Manu Singh and Tanu Singh "Prevailing issues and research confront in Underwater Acoustic Sensor Networks ", *International Journal of Computer Science and Information Technology & Security*, Vol.4,No.3,Jun.,2014.

[17]. M. Neugebauer, J. Ploennigs, and K. Kabitzsch, "Evaluation of Energy Costs for Single Hop vs. Multi Hop with Respect to Topology Parameters", *Factory Communication Systems, 2006 IEEE International Workshop on*, pp: 175-182, Torino, Italy, June, 2006.

[18]. M. Stojanavic, "On the Relationship Between Capacity and Distance in an Underwater Acoustic Communication Channel", *ACM WUWNet '06*, pp. 41 – 47, Los Angeles, CA, USA, Sept., 2006.

[19]. C. E. Perkins and P. Bhagwat, "Highly dynamic destination sequence distance vector routing (DSDV) for mobile computers," in *Proc. SIGCOMM'94*, Aug. 1994, pp. 234-244, London, UK.

[20]. V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *Proc. INFOCOM'97*, pp. 1405–1413, Kobe, Japan, Apr. 1997.

[21]. C. Zhang, M. C. Zhou, and M. Yu, "*Ad hoc* Network Routing and Security: A Review," *International Journal of Communication Systems*, Vol. 20, pp. 909-925, Aug. 2007.

[22]. Z. Wang, L. Liu and M. C. Zhou, "An Epidemic Routing Strategy for Vehicular Ad Hoc Wireless Networks in Intelligent Transportation Systems," *International Journal of Intelligent Control and Systems*, Vol. 10, No. 1, 86-93, March 2005.

[23]. C. E. Perkins, E. M. Belding-Royer and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing," *IETF Experimental RFC*, Jul. 2003.

[24]. Johnson DB, Maltz DA, Broch J. DSR: *the dynamic source routing protocol for multihop wireless ad hoc networks*. Ad hocnetworking. Addison-Wesley Longman Publishing Co., Inc; 2001. p. 139–72

[25]. Harris AR, Zorzi M. On *the design of energy-efficient routing protocols in underwater networks*. In: Proceedings of the 4th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks, SECON '07; 2007.

[26]. M. Ayaz, I. Baig, A. Abdullah, and I. Faye, "A survey on routing techniques in underwater wireless sensor networks," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1908– 1927, 2011.

[27]. D. Chen and P. K. Varshney, "A survey of void handling techniques for geographic routing in wireless networks," *IEEE Communications Surveys and Tutorials*, vol. 9, pp. 50–67, 2007.

[28]. U. Lee, P. Wang, Y. Noh, L. F. M. Vieira, M. Gerla, and J.-H. Cui, "Pressure routing for underwater sensor networks," in *Proceedings of the IEEE INFOCOM*, pp. 1–9,March 2010.

[29]. P. Xie, Z. Zhou, Z. Peng, J.-H. Cui, and Z. Shi, "Void avoidance in three-dimensional mobile underwater sensor networks," *Wireless Algorithms, Systems, and Applications*, vol. 5682, pp. 305–314, 2009.

[30]. P. Xie, J.-H. Cui, and L. Lao. VBF: Vector-Based Forwarding Protocol for Underwater Sensor Networks. In IFIP Networking , Coimbra, Portugal, May 15 - 19 2006.

[31].performance of computer and communication networks;mobile and wireless communication systems. Berlin/Heidelberg: Springer;2006a. p.1216-1221.

[32]. J. M. Jornet, M. Stojanovic, and M. Zorzi, "Focused beam routing protocol for underwater acoustic networks," in Proceedings of the third

ACM international workshop on Underwater Networks, ser. WuWNeT'08. New York, NY, USA: ACM, 2008, pp. 75-82.

[33].Daeyoup Hwang, Dongkyun Kim, "DFR: Directional flooding-based routing protocol for underwater sensor networks" IEEE OCEANS 2008, pp. 1-7, 2008.

[34].Wang, Y., Gao, J. and Mitchell, J. (2006) "Boundary recognition in sensor networks by topological methods," Proc. of ACM MobiCom, pp. 122–133.

[35].Fekete, S., Kroeller, A., Pfisterer, D., Fischer, S. and Buschmann, C. (2004) "Neighborhood-based topology recognition in sensor networks," Proceeding of First International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSOR), pp. 123–136.

[36].Chirdchoo, N., Wee-Seng, S. and Kee Chaing, C. (2009) "Sector-based routing with destination location prediction for underwater mobile networks", In Proceedings of the international conferenceon advanced information networking and applications workshops 2009, (WAINA '09), pp. 1148-1153.