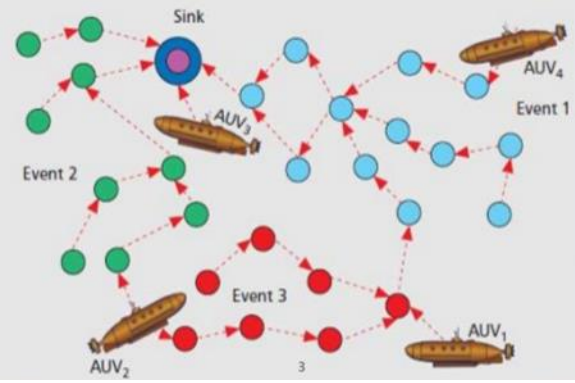
Comparison between under water wireless sensors and Terrestrial Wireless Sensors: A Review

Deepika D Pai
Asst.Professor (Selection Grade) Vemana Institute of Technology

***Abstract*- Wireless Sensor Networks (WSN) have recently commanded the attention of many researchers. However, when compared to terrestrial WSN, Underwater Sensor Networks (UWSN) present a novel-networking paradigm. The deployment of UWSN is challenging due to the type of environment found underwater. This paper provides a comparison of the two types of sensor networks. In addition, this paper proposes the possible research directions in this field.**

***Index Terms*- Wireless Sensor Networks(WSN), Underwater Wireless Communication Networks (UWCNS), Autonomous Underwater Vehicles (AUVS)**

I. INTRODUCTION



Underwater wireless communication is a form of wireless communication where acoustic waves carry the digital information through an underwater channel. Unlike the terrestrial waves which give more throughput at higher frequencies, under water the radio waves follow the principle of a higher loss of energy at higher frequencies resulting in a poor throughput. Acoustic waves are chosen as the best option because radio waves propagate under water at extremely low frequencies(30Hz-300Hz) and require large antennae and high transmission power, and optical waves are affected by scattering. Underwater wireless communication networks (UWCNs) are constituted by sensors and autonomous underwater vehicles (AUVs) that interact to perform specific applications such as underwater monitoring. These networks have to take care of the living beings in the ocean and take care not to harm them when using the sensors and AUV's.The Underwater Wireless Sensor Networks is made of three basic components which are:

•The sensors nodes: They are simply energy constrained devices that have ability of sensing the surrounding environment.

- Sink (Base Station): It is a more powerful node that behaves as an interface between the sensor nodes and the clients.
- Autonomous Underwater Vehicle: It is a marine technology that does not need any physical governance by any person while it is being put in the water. It operates on the basis of something known as the Underwater Acoustic Positioning System which uses the aid of the GPS fitted in the ship or the naval vessel to propel it further in the water.

There are certain challenges in the design of the underwater network, which are:

1. The available bandwidth is severely limited due to low carrier frequency.
2. The underwater channel is impaired because of multipath and fading.
3. Battery power is limited as the batteries cannot be recharged.
4. Underwater sensors are prone to failures because of fouling and corrosion.

The underwater sensor network is different from the terrestrial sensor networks in terms of cost, deployment, power, memory and spatial correlation. This makes the aquatic environment vulnerable to malicious attacks and hence require the development of efficient and reliable security mechanisms. Coordination and sharing of information between sensors and AUVs make the provision of security challenging. The aquatic environment is particularly vulnerable to malicious attacks due to the high bit error rates, large and variable propagation delays, and

low bandwidth of acoustic channels. Achieving reliable intervehicle and sensor-AUV communication is especially difficult due to the mobility of AUVs and the movement of sensors with water currents.

II. COMPARISON BETWEEN WSN AND UWSN

A.Comparison in terms of Architecture

Architecture of Terrestrial Communication System

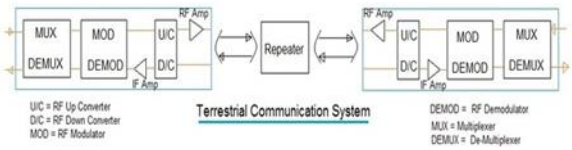


Fig 1: Terrestrial Communication System

The terrestrial sensor networks are designed to operate on the land and hence air is used as a channel for communication. A typical terrestrial sensor network is composed of transmitter and receiver part and uses electromagnetic radio waves for carrying the information (data or voice).

The figure-1 depicts terrestrial communication system with two stations and repeater module. Multiple repeaters are used between source and destination stations to receive the signal from one end and amplify and retransmit the signal to the other end. Hence repeaters will make up for the RF losses introduced due to path pass. Typically, repeaters are placed at the distance of about 32 to 80 Km.

Terrestrial system uses both analog and digital modulation types. In analog systems, data information signals are frequency multiplexed(FDM) first and later modulated (FM) and up converted for the transmission using RF antenna. In digital systems, data information signals are time multiplexed(TDM) to form baseband signal. This is later modulated (using either PM or PSK) and up converted for transmission using RF antenna.

Architecture of Underwater Communication System

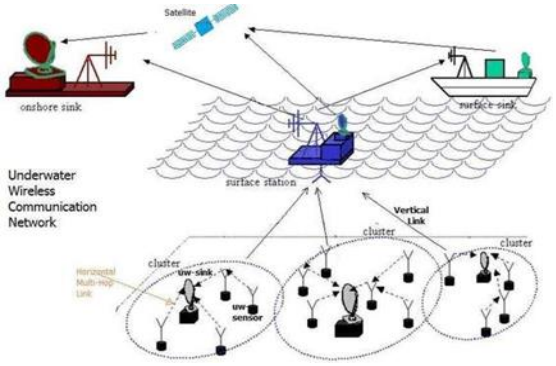


Fig 2: Underwater wireless communication network using acoustic waves

Figure-2 depicts centralized architecture of underwater communication system. As shown a group of sensor nodes are installed at the bottom of ocean which communicate with one or more underwater installed sinks(uw-sinks). These uw-sinks operate as relays between underwater nodes and surface station. As shown surface station communicates with surface sink and onshore sink using satellite links. Like land mobile communication, bottom area of ocean is divided into clusters. One uw-sink is installed or anchored in each of the clusters. In order to achieve communication with both underwater nodes and also with surface station, uw-sink is equipped with two transceivers namely horizontal and vertical.

The horizontal transceiver is a short-range transceiver which provides communication between uw-sink and sensor nodes. Commands/Configuration data is sent from uw-sink to sensors over these links. The sensors collect the monitored data from uw-sink using these links. The vertical transceiver is used for long range communication between uw-sink and surface station as shown. These transceivers can cover distance of up to 10 km.

B.Comparison in terms of Protocol stack

The protocol stack of the sensor network is much like the traditional protocol stack, with the following layers: application, transport, network, data link, and physical and is shown in the figure 3 below.

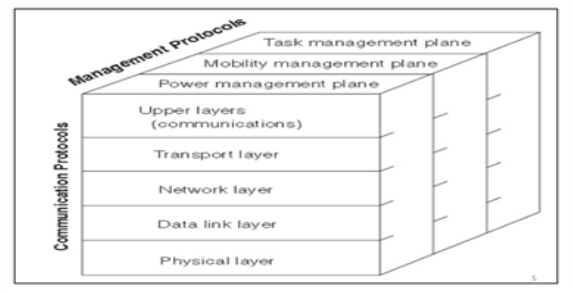


Fig 3: Protocol stack for WSN

Physical layer- is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption.

Data link layer- is responsible for the multiplexing of data streams, data frame detection, medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.

Network layer- takes care of routing the data supplied by the transport layer. The
network layer design in WSNs must consider the power efficiency, data-centric
communication, data aggregation, etc.

Transport layer- helps to maintain the data flow and may be important if WSNs are planned to be accessed through the Internet or other external networks.

Application layer- Depending on the sensing tasks, different types of application software can be set up and used on the application layer.

Power management plane - is responsible for minimizing power consumption and may turn off functionality in order to preserve energy.

Mobility management plane - detects and registers movement of nodes so that a data route to the sink is always maintained.

Task management plane- balances and schedules the sensing tasks assigned to the sensing field and thus only the necessary nodes are assigned with sensing tasks and the remainder are able to focus on routing and data aggregation

Protocol Stack for Underwater acoustic communication

The protocol stack of this system consists of four layers namely physical layer, datalink layer, network layer and transport layer. These layers have the same functionality as of OSI layers.

Physical Layer-This layer takes care of modulation and error correction. As phase tracking is a tedious task underwater, non-coherent FSK modulation is used in the modem used for the underwater communication system. Presently the advancement in DSP has led to the development of PSK and QAM based modems which are used for these underwater applications.

Datalink Layer- It is similar to MAC layer used for providing access of common resources to multiple nodes. The common techniques used for multiple access are FDMA, TDMA and CDMA.

Network Layer- This layer basically takes care of routing of messages within the network. The protocols depend on network topology employed in underwater network.

Transport Layer- This layer provides reliable communication between two systems (i.e. transmitting and receiving). It also takes care of flow control as well as congestion control.

C.Comparison with respect to the characteristics of the channel

Characteristics of Wireless Channel

The most important characteristics of wireless channel are −

- Path loss
- Fading
- Interference

Path Loss: It can be expressed as the ratio of the power of the transmitted signal to the power of the same signal received by the receiver, on a given path. It is a function of the propagation distance. Estimation of path loss is a very important factor for designing and deploying wireless communication networks and it is dependent on a number of factors such as the radio frequency used and the nature of the terrain. There are two path loss models to be considered:

i.The free space propagation model: It is the simplest path loss model in which there is a direct-path signal between the transmitter and the receiver, with no atmosphere attenuation or multipath components. In this model, the relationship between the transmitted power Pt and the received power Pr is given by

$Pr=PtGtGr(\lambda 4\Pi d)2$

Where Gt is the transmitter antenna gain, Gr is the receiver antenna gain, d is the distance between the transmitter and receiver and λ is the wavelength of the signal.

ii.Two-way model: It is also called as two path models and is the most widely used path loss model. The free space model assumes that there is only one single path from the transmitter to the receiver. Practically, the signal reaches the receiver through multiple paths, and the two-path model tries to capture this phenomenon. The model assumes that the signal reaches the receiver through two paths, one a line-of-sight and the other the path through which the reflected wave is received.

According to the two-path model, the received power is given by

$Pr=PtGtGr(hthrd2)2$

Where Pt is the transmitted power, Gt represent the antenna gain at the transmitter, Gr represent the antenna gain at the receiver, d is the distance between the transmitter and receiver, ht is the height of the transmitter and hr is the height of the receiver.

Fading: Fading refers to the fluctuations in signal strength when received at the receiver.

Fading can be classified in to two types −

- Fast fading/Small scale fading and
- Slow fading/Large scale fading.

Fast fading refers to the rapid fluctuations in the amplitude, phase or multipath delays of the received signal, due to the interference between multiple versions of the same transmitted signal arriving at the receiver at slightly different times.

The time between the reception of the first version of the signal and the last echoed signal is called 'delay spread'. The multipath propagation of the transmitted signal, which causes fast fading, is because of the three propagation mechanisms, namely −Reflection, Diffraction and Scattering. The multiple signal paths may sometimes add constructively or sometimes destructively at the receiver causing a variation in the power level of the received signal. The received single envelope of a fast fading signal is said to follow a Rayleigh distribution to see if there is no line-of-sight path between the transmitter and the receiver.

Slow Fading: The name Slow Fading itself implies that the signal fades away slowly. It is

also referred to as 'Shadow Fading' since the objects that cause the fade, which may be large buildings or other structures, block the direct transmission path from the transmitter to the receiver. Slow fading is so called because the duration of the fade may last for multiple seconds or minutes. Slow fading may occur when the receiver is inside a building and the radio wave must pass through the walls of a building, or when the receiver is temporarily shielded from the transmitter by a building. The obstructing objects cause a random variation in the received signal power. Slow fading may cause the received signal power to vary, though the distance between the transmitter and receiver remains the same.

Interference: Wireless transmissions have to counter interference from a wide variety of sources. Two main forms of interference are −Adjacent channel interference and Co-channel interference.

In the case of Adjacent channel interference, signals in nearby frequencies have components outside their allocated ranges, and these components may interfere with on-going transmission in the adjacent frequencies. It can be avoided by carefully introducing guard bands between the allocated frequency ranges.

Co-channel interference, is sometimes also referred to as narrow band interference, is due to other nearby systems using the same transmission frequency.

Inter-symbol interference is another type of interference, where distortion in the received signal is caused by the temporal spreading and the consequent overlapping of individual pulses in the signal. Adaptive equalization is a commonly used technique for combating inter symbol interference. It involves gathering the dispersed symbol energy into its original time interval. Complex digital processing algorithms are used in the equalization process.

Characteristics of the Underwater Channel

Underwater acoustic communications are mainly influenced by:

- Transmission Loss
- Noise
- Multipath
- Doppler Spread
- High and Variable Propagation Delay.

All these factors determine the temporal and spatial variability of the acoustic channel, and make the available bandwidth of the underwater acoustic channel limited and dramatically dependent on both range and frequency. Long-range systems that operate over several tens of kilometers may have a bandwidth of only a few kHz, while a short-range system operating over several tens of meters may have more than a hundred kHz of bandwidth. In both cases, these factors lead to low bit rate, in the order of tens of kbps for existing devices. These factors are explained below:

Transmission loss: It consists of attenuation and geometric spreading, where the attenuation is mainly caused by absorption due to conversion of acoustic energy into heat and the geometric spreading is caused by the spreading of sound energy as a result of the expansion of the wave fronts.

Noise: It can be classified as man-made noise and ambient noise.

Multipath: Multipath propagation is responsible for severe degradation of the acoustic communication signal, since it generates Inter Symbol Interference (ISI).

Doppler spread: The Doppler frequency spread can be significant in underwater channels, causing a

degradation in the performance of digital communications.

High delay and delay variance: The propagation speed in the underwater channel is five orders of magnitude lower than in the radio channel.

D.Attacks and countermeasures in WSN and UWSN

The Table below shows the Mapping of Security Attacks on Layers of Protocol Stack.

Layers of Protocol Stack	Attacks	Protection measures
Physical Layer	Jamming, Node Replication	Temper-proofing, Spread Spectrum, hiding, Duty cycle region mapping
Data Link Layer	Jamming, Collision, Exhaustion	Tiny Sec, Error correcting code, Link Layer Encryption, Distributed MD(mediation device) protocol.
Network Layer	Neglect or Selective forwarding, Sybil, Wormhole, Spoofing, Homing, Sink or Black holes, Hello-Flooding	TIK based upon symmetric cryptography, Multipath Routing, REWARD algorithm, SNEP.
Application Layer	Data Aggregation, Desynchronization	SDAP, Aggregate commit-prove Framework

Table 1: Mapping of Security Attacks on Layers of Protocol Stack

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.

i.Jamming attack: It is a type of attack which interferes with the communication protocols of the physical channel, by putting noises or meaningless signals at the nodes used in a UWSN for communication. A jamming source may be powerful enough to disrupt the entire network, when an attacker intently jams 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 which are:

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

i.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 refills them into the network.

Counter measures

It can be overcome using following two techniques are:

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

ii.Sinkhole Attack: In a sinkhole attack, a malicious node attempts to provide a false routing information to other nodes, and produce itself as the intended 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.

Counter measures

It can be overcome using following two techniques are:

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

iii.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

iv.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.

v.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.

Counter measures

It can be overcome using following two techniques are:

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

vi.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

1.Encryption of all packets sent through the network.

III.CONCLUSION

Underwater wireless sensor networks (UWNS) will become more and more important on the research of underwater world. This paper describes the unique characteristics of the underwater environment and its effects on the design of UWSN. In addition, the differences between terrestrial WSN and UWSN are presented. Even though they are different, terrestrial WSN is still valuable on UWSN.

REFERENCES

[1] Akildiz, I.F., Pompili, D., Melodia, T., Underwater Acoustic Sensor Networks: Research Challenges, Ad Hoc Networks,3, (260), 2005.

[2] Kifoyle, D.B., Baggeroer, A. B., The State of the Art in Underwater Acoustic Telemetry, IEEE J. Oceanic Eng., (OE-25, no. 5), 4-27, Jan. 2000.

[3] Etter, P. C., Underwater Acoustic Modeling, Principles, Techniques and Applications. 2nd edition, E&FN Spon, 1996.

[4] Berkhovskikh, L., Lysanov, Y., Fundamentals of Ocean Acoustics, New York: Springer, 1982.

[5] Proakis, J., Rice, J., Sozer, E., Stojanovic, M., Shallow water acoustic networks, Encyclopedia of Telecommunications, Proakis, J. G., Ed. John Wiley and Sons, 2003.

[6] Knudsen, V.O., Alford, R.S., Emling, J.W., Digital Communications. Marine Research (7-12), 410, 1948.

[7] Cui, J.H., Kong, J., Gerla, M., Zhou, S., The Challenges of Building Scalable Mobile Underwater Wireless Sensor Networks for Aquatic Applications, IEEE Network, (0890-8044), 12-17, May/June 2006.

[8] Vasilescu, I., Kotay, K., Rus, D., Krill: An Exploration in Underwater Sensor Networks, Second IEEE Workshop, (30-31), 151-152, May 2005.

[9] Biswas, P., Ye, Y.Y., Semidefinite programming for ad hoc wireless sensor network localization, Proceedings of the third international symposium on Information processing in sensor networks, (46-54), April 2004.

[10] International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.1, Pages: 05 – 11 (2015)

[11] Special Issue of ICEEMC 2015 - Held during January 27, 2015, Chennai, India

[12] M.Kiranmayi, Dr. Kathirvel Ayyaswamy Underwater Wireless Sensor Networks: Applications, Challenges and Design Issues of the Network Layer -A Review

[13] International Journal Of Multidisciplinary Sciences And Engineering, VOL. 5, NO. 5, MAY 2014[ISSN: 2045-7057] www.ijmse.org
[14] Muhammad Ahsan Raza1, Binish Raza and Anum Aftab Comparative Study of Security Attacks on Wireless Sensor Networks.
[15] www.rfwireless-world.com/.../terrestrial-sensor-network-vs-underwater-sensor-networ...