RESEARCHERID
THOMSON REUTERS

[COTII- 2018] ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

CHALLENGES, PROSPECTS AND SECURITY IN UNDER WATER WIRELESS COMMUNICATION

Anant Sinha[a], Sachin Kumar[b], Sumita Mishra[c] & Pallavi Asthana[d]
(Department of Electronics and communication Engineering, Amity University, Lucknow

ABSTRACT

Underwater wireless communications refers to the transmission of data in an unguided water environment through wireless devices. Underwater wireless communications play a vital role in various marine activities like environmental monitoring, underwater exploration, defense and scientific data collection. Wireless communication under water owing to unpredictable conditions is still a challenging task, such as sensor failure due to corrosion, severe attenuation, multipath dispersion, data insecurity etc. Mobile communication utilizes frequency range of 800-1900 MHz, frequencies in this range are extremely high to travel in water, hence communication under water is achieved through Extreme low frequencies (3Hz-30Hz), Super low frequencies (30Hz-300Hz) and very low frequencies (3KHz-30KHz), due to very large wavelength these waves can easily travel in water but the transmission and reception of these waves is not easy, it requires specific antennas of very large size which consumes more power. Another disadvantage is that these frequencies offers small bandwidth hence data transmission speed is very slow (200-300 Bits/sec). This paper presents more advanced techniques to overcome the flaws of existing technology. One of the technique is Quantom Keying Distribution (QKD). This techniques is much secure as compared to other communication techniques.

Keywords: *Wireless communication, Acoustic wave, optical communication, Electromagnetic communication Quantum key distribution.*

I. INTRODUCTION

Today everything in the world is connected by wireless technologies, whether it is on the Earth surface or in the space. Astonishingly, an important frontier is omitted, which occupies 70% of our planet, where wireless technology is not efficient so far, this is the underwater world, 95% of which is still not explored.. It is peculiar that we are able to communicate with Satellite (Voyager-1, ~10^{11}km away from earth) using few watts of power (18Watts in the high power mode), but we do not have proficient communication system with our submarines lying few meters down the sea, in spite of the fact that we are providing megawatts of power in the ELF/VLF facilities for one way communication with submarines [1].

During the past era, underwater wireless communication have involved significant interests from both academia and industry due its wide range of applications including in the military, industry, and the scientific community, it plays a dynamic role in tactical surveillance, pollution monitoring, offshore explorations, climate change monitoring, and oceanography research. To carry out such activities there is a rise in the number of Unmanned Vehicles or devices which are installed under water, such devices require large bandwidth and capacity for data transmission [2].

At present following three technologies are used in underwater wireless communication [3]:

- Acoustic wave communication (ACOMM)
- Underwater Optical wireless communication (UOWC)
- Electromagnetic communication (EMCOMM)

The section II of this paper covers all the three technologies in detail along with the challenges encountered during their application. Section III deals with security issues and conclusion is presented in section IV.

II. EXISTING TECHNOLOGY

A. Acoustic wave communication (ACOMM)

An Acoustic wave Sensor is an electronic device which is capable of measuring the level of sound. When an Acoustic wave travels through a certain medium, it is highly affected by properties of medium and the obstacles appear in its path. Acoustic waves also called sound waves are used due to low absorption in underwater environment. In Acoustic wave communication Pulses of sound travel between underwater sensor nodes distributed a few kilometers apart. To connect with terrestrial technologies, the nodes communicate with gateway buoys (floating devices) on the water's surface, linking to the above-sea internet via cellular networks or satellites [4]. The present underwater acoustic communication can support data rate up to tens of kbps for long distances (ranging in kms) and up to hundreds of kbps for short distances (few meters). Acoustic communication can be categorize on the basis of distance and bandwidth as shown in table 1 [5].

TABLE 1 :Bandwidth requirement for Acoustic under water communication

Link Type	**Range in Km**	**Bandwidth in KHz**
Very Long	1000	< 1
Long	10 to 100	2 to 5
Medium	1 to 10	~10
Short	0.1 to 1	20 to 50
Very Short	< 0.1	>100

Some major challenges in Acoustic wave communication are as following:

- Networks which are designed for rapid ratification and communication are not operated and will “time out” waiting for responses. This is because acoustic signals propagates much slowly than radio waves, takes about two seconds to travel back and forth across a distance of 1.5 kilometers [6].

- Signal propagation is influenced by refraction absorption, and scattering through the water. Attenuation is greater in liquid compared to air. With acoustics, there is a very high reflection of signals underwater. There are numerous ways to get reflections such as the signal can bounce off the seafloor and other underwater rocks or structures, including softer mediums such as the ocean’s surface and layers of water separated by differences in temperature or density. Multipath propagation is shown in figure 1 [7].

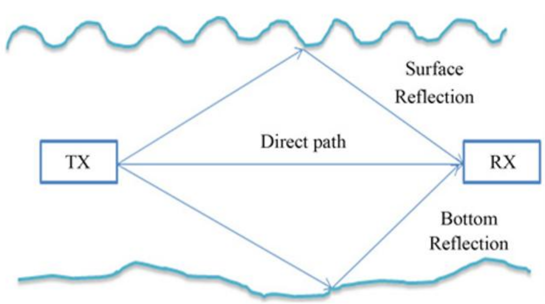

Fig 1: Multipath Propagation Underwater

- Localization plays a noteworthy role in underwater sensors. It is also a significant issue for data tagging and making routing decisions. Localization techniques employed for ground-based sensor networks cannot be used for underwater communication because of long propagation delays, Doppler Effect, multipath etc. [8]

B. Optical wave communication

Since RF signals require an antenna of huge size, large transmitter power in fresh water and experience high attenuation in sea water, the another obvious choice for underwater wireless communication is optical signal. Optical wireless communication utilize modulated optical beams in order to establish short, medium or long communications [9]. The major advantages of using optical wave for communication are [10]:

- High data rate that can exceed up to 1 Gbps at a few hundred meters of distance due to high frequency of optical carrier.
- Optical waves acquire high propagation speed in underwater environment, hence optical transmission does not practically suffer from latency.
- Optical communication system requires low installation and operation costs also have light weighted transceiver.
- There is no need of licensing fees and tariffs, because optical band is not a part of the telecommunications regulations.

A major challenge in underwater optical wireless communication is:
When light propagates in water, the photon interacts with the water molecules and with other particulate matters inside the water. This interaction results in absorption and scattering which attenuate the transmitted optical signal [11].

However, it is observed from the studies that blue/green region of the visible spectrum are least absorbed in Sea water. Thus, using appropriate wavelengths, for instance in the blue/green region, high speed connections can be achieved according to the type of water (400–500 nm for clear to 300–700 nm for turbid water conditions). Minimum attenuation is centered near 0.460 µm in clear waters and shifts to higher values for dirty waters approaching 0.540 µm for coastal waters. [12]

C. Electromagnetic communication (EMCOMM)

The major challenge in using radio waves in underwater is the severe attenuation due to the conducting nature of seawater, due to which EMCOMM works in the power-limited region**.** Extremely low frequency (ELF) radio signals have been used in military applications. (ELF) signal, typically around 80 Hz at much lesser power, has been used in communication with naval submarines across the World today. As depicted in figure 2 it is observed from the studies that RF frequencies in MHz range are proficient of propagating in sea water up to distance of 100 m by utilizing dipole radiation with high transmission power of about 100 W. However, it requires more sophisticated antennas design and high transmission power [13]. Table 2 summarizes the comparative merits and drawbacks of three major techniques of underwater communication.

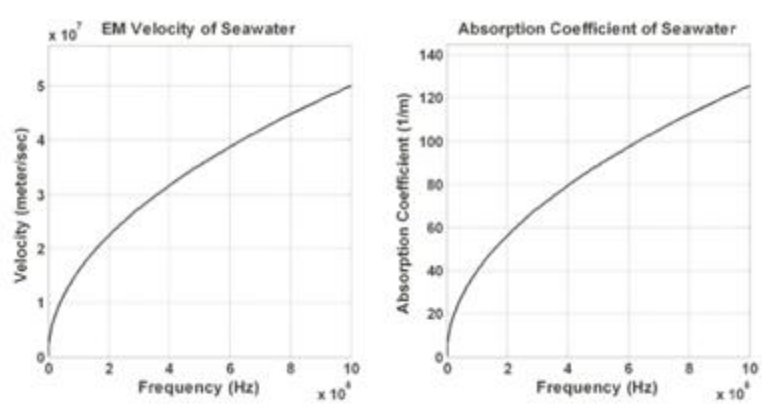

Fig 2: Velocity and absorption versus frequency for EM waves in seawater [14].

ISSN 2348 – 8034
Impact Factor- 5.070

TABLE 2 The comparative study of three techniques for underwater wireless communication

Parameter	Acoustic	RF	Optical
Attenuation	Distance and Frequency dependent (0.1-4dB/Km)	Frequency and conductivity dependent (3.5-5 dB/m)	0.39 dB/m-11 dB/m
Speed (m/s)	1500m/s	2255 x 10^8	2.255 x 10^8
Data Rate	~Kbps	~Mbps	~ Gbps
Latency	High	Moderate	Low
Distance	Up to Kms	10 meters	10-100 meters
Bandwidth	Distance dependent 1000Km< 1KHz 1-10Km ~ 10KHz <100m~ 100KHz	~MHz	10-150 MHz
Frequency band	10-15KHz	30-300 Hz (ELF)	10^{12}-10^{15}
Transmission Power	Tens of Watts	Few mW to hundreds of Watts	Few Watts
Antenna Size	0.1m	0.5 m	0.1 m
Efficiency	100bits/Joule		30,000bits/Joule
Performance Parameters	Temperature, salinity and pressure	Conductivity and Permittivity	Absorption, Scattering

III. SECURITY ISSUES IN UNDERWATER ACOUSTIC COMMUNICATION

- **Jamming:** Jamming attacks use the carriers of neighboring frequency nodes to interfere with the medium. Underwater communications networks are susceptible to narrowband jamming. The attacker can jam the communication between a sender and a receiver and later they can retrieve and manipulate the information [16].
- **Wormhole Attack:** Hackers create wormhole between two physical locations in a network. In such case, the malicious node transfers some specific packets and injects them into the network. As a result of which, false neighbor relationships are established, as two nodes out of each other's range can mistakenly conclude that they are in proximity with one another due to the wormhole's presence [16].

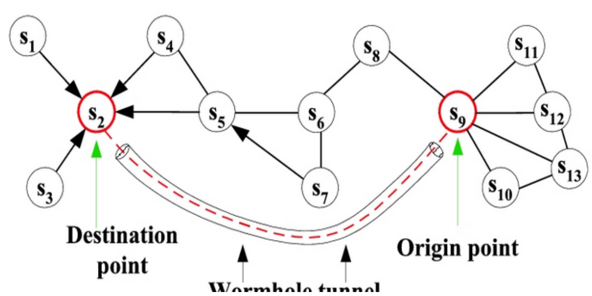

Fig 3 Wormhole Attack

- **Sinkhqole Attack**: In the Sinkhole Attack malicious node attempts to attract traffic from a particular area. Geographic routing and authentication of nodes using routing information are possible fortifications against this attack, but it is an unexplored area so far [17].

- **Hello Flood Attack**: Every New node broadcast a "Hello" message to find its neighbors. Other nodes may route their data through these new nodes if the path is shorter, hackers take the advantage of this thing, a node when receives a "Hello" message from a malicious node, it may interpret that it is from some neighbor [17].
- **Sybil Attack:** An attacker with multiple identities can pretend to be in many places at same time. Authentication and position verification can be helpful but difficult to check due to mobility [17].

A. Security Requirement's for underwater wireless communication [17]

- **Authentication:** It shows that the data was sent by a authorized sender. It is mainly essential in defense applications. surveillance
- **Confidentiality:** It ensures that information is not accessible any unauthorized party. Thus, more emphasis should be given to the confidentiality of applications such as maritime surveillance.
- **Integrity:** Any intruder should not be able to manipulate the information. Many underwater sensor applications such as water quality monitoring require highly reliable information.
- **Availability:** It suggests that the information could be retrieved easily when required by an authorized user. Any time lag would affect critical aquatic exploration applications like prediction of sea quakes

B. Quantum Keying Distribution (QKD) for secure underwater communication

In recent years quantum communication or QKD has made a great advancement in both theoretical and practical experiments across the word. Quantum key distribution make use of fundamental laws of Quantum Physics to secure the information. It makes data completely immune from hackers attack. In a Quantum channel a single Photon carries information which changes irreversible when someone attempts to interrupt it, hence users instantly get the information of attack. It allows two parties to produce a shared random secret key which is known only to them, that can be used to encode and decode messages. It is also known as called quantum cryptography. It should be noted that Quantum key distribution is utilized only to produce and distribute a key, not for data transmission. This key can then be used with any chosen encryption algorithm to encode and decode a message, which can then be transmitted over a standard communication channel [18].

IV. CONCLUSION

An enhancement is required in underwater wireless communication system due to increased number of unmanned vehicles in underwater. Traditional underwater communication is associated with acoustic signals and despite the substantial advancement in this area, acoustic communication systems are not that much efficient to fulfill present communication requirements. It is observed from the study that though acoustic waves are the robust and feasible carrier in today's scenario but with rapid technological development and active ongoing research is in UOWC, this technology will be more promising with game-changing potentials in the near future. Underwater wireless communication networks are particularly susceptible to malicious attacks due to the high bit error rates, large and variable propagation delays, and low bandwidth of acoustic channels. Various security issues like jamming can be resolved by using optical communication systems.

REFERENCES

1. Davide Anguita, Davide Brizzolara, Giancarlo Parodi "Optical communication for Underwater Wireless Sensor Networks "OCEANS 2009 - EUROPE 11-14 May 2009
2. M. Stojanovic, ''Recent advances in high-speed underwater acoustic communications,'' IEEE J. Ocean. Eng., vol. 21, no. 2, pp. 125–136, Apr. 1996.
3. S. Arnon, ''Underwater optical wireless communication network,'' J. OptEng., vol. 49 no. 1, pp. 015001-1–015001-6, 2010.
4. I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: Research challenges," Ad Hoc Networks, pp. 257–279, 2005.
5. Akyildiz, I.F.; Pompili, D.; Melodia, T. Challenges for efficient communication in underwater acoustic sensor networks. ACM Sigbed Rev. 2004, 1, 1–6.

6. Liu, L.; Zhou, S.; Cui, J.-H. Prospects and problems of wireless communications for underwater sensor networks. Wirel. Commun. Mob. Comput.-Spec. Issue Underw. Sens. Netw. 2008, 8, 977–994.
7. Stojanovic M. Underwater wireless communications: Current achievements and research challenges. IEEE Oceanic Engineering Society Newsletter. 2006; 41(2):10–3.
8. Kasture S, Gudpelliwar N. Securing underwater wireless communication networks-literature. International Journal of Scientific and Engineering Research. 2013; 4(12):73–8.
9. Z. Ghassemlooy and W. O. Popoola, Terrestrial Free-SpacemOptical Communications. .Rijeka, Croatia: InTech, 2010, ch. 17, pp. 356–392.
10. M. A. Khalighi and M. Uysal, ''Survey on free space optical communication: communication theory perspective,'' IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 2231 2258, Nov. 2014.
11. Stojanovic M. Underwater wireless communications: Current achievements and research challenges. IEEE Oceanic Engineering Society Newsletter. 2006; 41(2):10–3.
12. Jurdak R, Lopes CV, Baldi P. A survey, classification and comparative analysis of medium access control protocols for ad hoc networks. IEEE Communications Surveys and Tutorials, 2004; 6(1):2–16.
13. Stojanovic M, Catipovic J, Proakis J. Phase coherent digital communications for underwater acoustic channels. IEEE Journal of Oceanic Engineering. 1994; 19(1):100–11.
14. Z.Guo, G.Colombi,B. Wang,J.-H.Cui, D.Maggiorini, and G.P.Rossi,"Adaptiveroutingin underwaterdelay/disruption tolerantsensor networks," in Proceedings of Fifth IEEE/IFIP Annual Conference on Wireless On demand Network Systems and Services (WONS'08), Jan. 2008.
15. Hemani Kaushal, Georges Kaddoum " Underwater Optical wireless communication" International Conference IEEE 2016.
16. Kasture S, Gudpelliwar N. Securing underwater wireless communication networks-literature. International Journal of Scientific and Engineering Research. 2013; 4(12):73–8.
17. Raju KG, Kumar AV, Kumar GA, Kiran VR. Attacks and securing under water wireless communication networks. International Journal of Research in Advent Technology. 2014; 2(5):12–5.
18. V. Padamvathi, B. Vishnu Vardhan "Quantum Cryptography and Quantum Key Distribution Protocols "Advanced Computing (IACC), 2016 IEEE 6th International Conference.