Marine Information Technology

Curriculum Report

Title： Underwater Acoustic Communication Networks

Name： Hussain Ahmad Faraz

Student Number： 11934070

Major： Marine Information & Technology

I declare that the assignment here submitted is original except for source material explicitly acknowledged, and that the same or related material has not been previously submitted for another course. I also acknowledge that I am aware of University policy and regulations on honesty in academic work, and of the disciplinary guidelines and procedures applicable to breaches of such policy and regulations.

Signature:

Date:04/06/2020

UNDERWATER ACOUSTIC COMMUNICATION NETWORKS

CONTENTS:

- INTRODUCTION……..... (1)
- UNDERWATER SENSOR NETWORKS ARCHITECHURE…… (2)
- BASICS OF ACOUSTIC COMMUNICATION……. (4)
- OFDM…… (5)
- THREATS AND CHALLENGES……. (7)
- SECURITY REQUIREMENTS……..... (8)
- SECURITY ISSUES OF UWSNs……..… (9)
- CONCLUSION……. (11)
- REFRENCES…… (12)

UNDERWATER ACOUSTIC COMMUNICATION NETWORKS

INTRODUCTION:

Underwater wireless communications have assumed a very vital role in marine activities for military and commercial purposes. Some of these fields include environmental monitoring, underwater mining, subsea oil and gas, as well as the collection of scientific and oceanographic data. Underwater wireless communication networks (UWCNs) include the connection, synchronization and reticulation of information between nodes to perform functions for sensing and monitoring. As such, oceans cover 71 percent of the earth 's surface, there is a wide range of applications that are relevant to the UWCN (Underwater Communication Network). Some of these applications include coastal surveillance systems, autonomous underwater vehicle (AUV) operation, environmental research, connecting submarines to land, collecting data for autonomous oil-rig maintenance monitoring of water, among many others. Similar to the terrestrial internet one can predict the future importance of UWCN as we explore the oceans.

The signals that are used to carry digital information through an underwater channel are not radio signals, as electro-magnetic waves propagate only over extremely short distances. Acoustic communication is characterized by the use of acoustic signals as methods of communication from one point to another. Acoustic signal is the only technically feasible device that operates underwater. Owing to the high attenuation and absorption effect in underwater environment, electromagnetic wave can only travel in water with a limited distance compared to it. The absorption of electromagnetic energy in sea water is found to be around 45 f dB per kilo meter, where f is a frequency in Hertz. Conversely, the absorption of acoustic signal is around three orders of magnitude lower than most value frequencies. There are some inquiries into the use of optical signal for applications underwater. They do note, however, that the optical signal can only pass through small range in an area of very clean water (for example, deep water). It is therefore not a good resource for underwater long-distance transmission, even in a not-so-clean water, e.g., shallow water, climate. Underwater Acoustic Networks, including but not limited to Underwater Acoustic Sensor Networks (UASNs) and Autonomous Underwater Vehicle Networks (AUVNs), are defined as networks consisting of more than two nodes that use acoustic signals to communicate for applications underwater. UASNs and AUVNs are two major forms of UANs. The former consists of multiple sensor nodes, primarily for a supervising purpose. Typically, the nodes are without or with minimal movement capability. The latter is composed of high mobility autonomous or unmanned vehicles, deployed for mobility-needed applications, e.g. exploration. A UAN can be a UASN, or an AUVN, or a mix of both.

Typical physical layer technology in underwater networks is acoustic communication. In fact, radio waves only propagate at extra low frequencies (30-300 Hz), which require large antennas and high transmission power, at long distances via conductive sea water. Optical waves do not suffer from such high attenuation but are affected by scattering. Thus, links in underwater networks are based on acoustic wireless communications [1]. The traditional approach for ocean-bottom or ocean column monitoring is to deploy underwater sensors that record data during the monitoring mission, and then recover the instruments [2]. This approach has the following drawbacks:

- Onshore control systems and the monitoring instruments cannot communicate. This impedes any adaptive tuning of the instruments nor can the device be reconfigured after unusual events occur.
- The amount of data that can be collected by each sensor during the monitoring mission is limited by the capacity of the storage devices onboard (memories, hard disks, etc.).
- When errors or misconfigurations occur, they cannot be visible until the devices are recovered. It can quickly lead to a control mission failing entirely.
- Surveillance in real time is not possible. It is particularly important in applications such as seismic monitoring, in surveillance or environmental monitoring. The collected data cannot be retrieved before the instruments are restored, which may come several months after the monitoring mission begins.

Therefore, underwater networks need to be implemented which will enable real-time monitoring of selected ocean areas, remote configuration and contact with onshore human operators. This can be accomplished by linking underwater instruments by means of acoustic communication dependent wireless links. A lot of researchers are currently working to develop networking Ad hoc terrestrial wireless solutions and sensor networks. Although there are many recently developed networks protocols for wireless sensor networks, the unique features of the underwater acoustic communication channel, such as limited bandwidth

capacity and variable delays, require new data communication protocols that are very effective and reliable. The main differences can be addressed between terrestrial and underwater sensor networks:

- Leading to increased distances and more complex signal processing at the receivers, greater power is needed in underwater communications.
- In underwater networks, the deployment is considered to be sparser.
- Underwater sensors are more costly than ground sensors.
- While the readings from terrestrial sensors are often correlated, due to the higher distance between sensors this is more unlikely to happen in underwater networks.

Major challenges to Underwater Acoustic Networks design are:

- Underwater sensors are prone to failures due to fouling, corrosion, etc.
- Channel features including long and variable delays in propagation, multipath and fading problems.
- Battery capacity is minimal, and batteries cannot typically be recharged, even because solar power cannot be used.
- The bandwidth available is severely constrained [3].
- High bit error rates.

UNDERWATER SENSOR NETWORKS ARCHITECHURE:

The physical layer of the underwater network makes use of acoustic communication technologies. Acoustic technology features restricted bandwidth, power, and variable delays. Therefore, for underwater acoustic networks, new data communication techniques and effective protocols are needed. Designing the topology of the network requires tremendous commitment from the designer, since efficiency of the underwater network is usually dependent on topology design. Reliability of the network should increase with efficient network topology, and with less efficient topology, reliability of the network should also fall. Energy consumption of efficient network topology is much less than underwater network topology design is incorrect and less efficient. Underwater sensor networks can be divided into two main categories:

Two-Dimensional Underwater Sensor Networks:

Deep ocean anchors are used in the two-dimensional underwater sensor network architecture for collection of sensor nodes as shown in figure 1. Anchored nodes underwater use acoustic connections to communicate with each other or with the sinks underwater. Underwater sinks, using surface stations, are responsible for gathering data from deep ocean sensors and delivering it to offshore control stations. For this purpose, in the company of horizontal and vertical acoustic transceivers underwater sinks are provided. Horizontal transceivers are intended to communicate with the sensor node, collect data or provide commands as provided by the offshore command station, while vertical transceivers are used to transmit data to the command station. Because the ocean can be as deep as 10 km, there should be enough range for vertical transceivers. The surface sink equipped with acoustic transceivers has the ability to handle simultaneous communication through multiple underwater sinks that are coordinated. The surface sink is also designed to communicate with offshore sinks via comprehensive radio frequency transmitters [4-7].

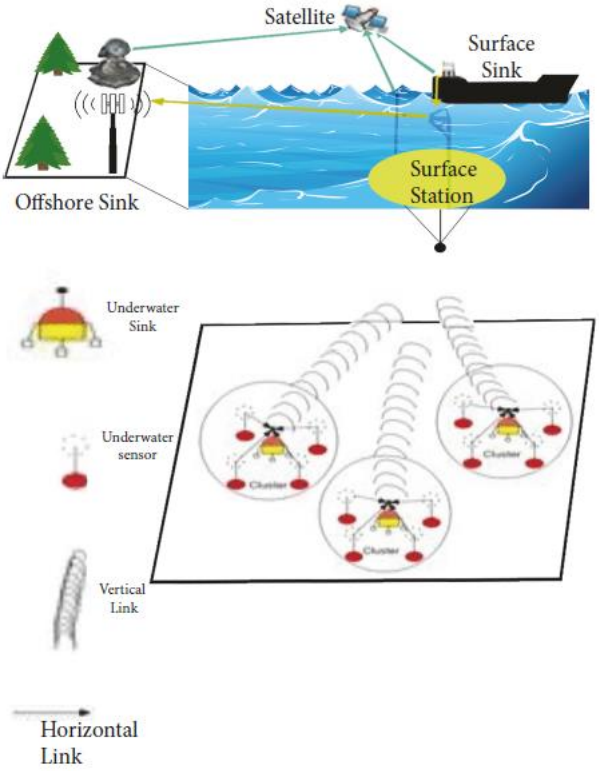

Fig. 1 Two-Dimensional Underwater Sensor Networks Architecture [5]

Three-Dimensional Underwater Sensor Networks:

Work needed to introduce new infrastructure in three-dimensional environments known as tridimensional networks underwater is used as shown in figure 2. In three-dimensional underwater networks, sensor nodes float at various depths to track a particular operation. Traditional solution for three-dimensional sensor networks underwater is the use of surface buoys that allow these network deployments. The solution, however, is susceptible to weather and manipulation. In the military action case, enemies can also easily discover and disable it. In architecture of three-dimensional sensor networks underwater, the ocean bottom is used to form anchored sensor nodes. The depth of these nodes is managed by means of wires connected with these anchors. The current properties of the oceans are influenced by major challenges concerning such networks [4-6].

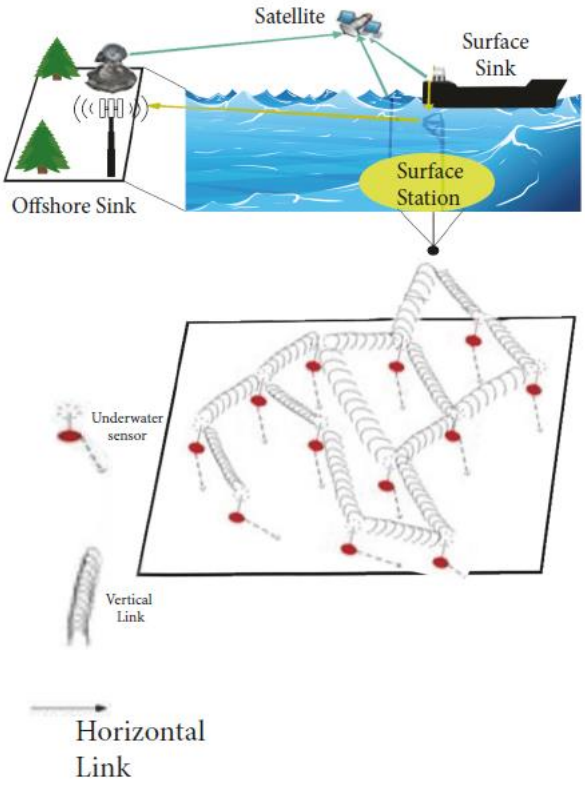

Fig. 2 Three-Dimensional Underwater Sensor Networks Architecture [5]

BASICS OF ACOUSTIC COMMUNICATION:

Underwater acoustic communication is a dynamic phenomenon since several environmental factors influence acoustic communication. These factors are complex, such as long delays in propagation, environmental noise, loss of direction, spread of Doppler and impact of multipaths. Underwater environmental factors make acoustic channel highly variable. They also establish bandwidth dependency between two nodes, on both frequency and distance. Ocean is usually divided into two parts; these are deep and shallow oceans. Shallow ocean highly affects the acoustic channel as compared to deep ocean due to high temperature gradient, multipath effect, surface noise and large delays in propagation. Underwater environment major propagation factors that affect acoustic communication are described below:

(1) **Path Loss:** When sound is propagated from the underwater environment, some of its strength becomes heat. The energy loss of sound wave propagation can be divided into three major categories listed below.

i. **Geometrical Spreading Loss:** As source produces acoustic signal it propagates in the form of wave fronts away from the source. This is therefore independent of frequency depending on the area reached by the origin of the wave. Geometric diffusion is divided into two types: first spherical spreading depicting deep ocean contact; second cylindrical spreading depicting shallow contact with water [8].

ii. **Attenuation:** Attenuation is characterized as "wave energy converted into some other type of energy" such as heat energy, which is absorbed by the medium. This phenomenon is sensitive in acoustic contact, as the heat is transformed into acoustic energy. The heat turned is absorbed by surrounding underwater. Attenuation is instant proportional of reach and frequency.

iii. **Scattering Loss:** Deviation with respect to the signal line of sight or angle shift is usually a physical property. Underwater channel also contains this property which affects the transmission of data from the acoustic channel during communication. Surface roughness increases due to wind increase velocity. That elevates the surface dispersing end product. Surface scattering causes not only delays but also power loss.

(2) **Noise:** Noise can be characterized as a communication system quality which will degrade the signal strength of any communication system. Various types of noises occur in the case of underwater acoustic channels. Underwater noises can be divided into two major categories.

i. **Human Made Noise:** Such noises are triggered by heavy machinery use, shipping activities, fishing activities, military operations, sonar operations, and aircraft activities, and the sending and receiving of heavy data traffic activity causes various forms of disturbance and interference during acoustic communication. Noise attributable to humans often even disturbs normal acoustic contact.

ii. **Ambient Noise:** Ambient noise is a complex phenomenon concerning communication underwater. It can also be characterized as a combination of different sources, which cannot be described uniquely [9]. Ambient noise is also called background noise attributable to unidentified sources. These noises are grouped into four essential categories called wind, shipping, heat and turbulence [10]. Wind noise is caused by breakage of wave or because of bubbles created by air. Noise can be simply predicted and forecast from weather forecasts because of dependence of noise upon wind speed. Large number of ships present at large distance from communication system in ocean produce high traffic noise in acoustic communication, if sound propagation is good enough. Ships consider primary source of anthropogenic ambient noise. Turbulence can be defined as surface disturbance due to waves or tides that generate low frequencies that result in acoustic communication with continuous noise. Underlying noise is regarded as thermal noise in lack of all other sources of noise, even self-noise. Thermal noise is proportional to the frequency used for acoustic communication [11].

(3) **Multipath:** Multi-path propagation can be responsible for significant deterioration of the acoustic signal, because it produces inter-symbol interference (ISI). The geometry of multipaths depends on the configuration of the connections. Vertical channels are distinguished by a small-time dispersion, while horizontal channels can have extremely long multi-path intervals, the value of which depends on the depth of the water.

(4) **High Delay and Delay Variance:** In the UW-A channel the transmission speed is five orders of magnitude lower than in the radio system. This large delay in propagation (0.67 s / km) will significantly reduce network throughput. The very high delay variance is even more harmful for efficient protocol design, as it prevents from accurately estimating the round-trip time (RTT), key measure for many common communication protocols.

(5) **Doppler Spread:** Because of channel flaws, wireless signals practice a diversity of degradations. For example, electromagnetic signal affects by interference, reflections, and attenuation; underwater acoustic signals are also affected by the same factors [12]. Due to time variation and space variation the underwater acoustic channel is a complex channel. Doppler shift is called the relative motion of transmitter and receiver which causes the mean frequency shift. Though the frequency fluctuation in this Doppler shift region is called Doppler spread. Two types of influences are observed on acoustic channel because of Doppler Effect: first is pulse width that will be compressed or stretched and second is frequency offset as a result of frequency offset compressing or expending of signal time domain occurring [13].

OFDM for Underwater Acoustic Channel:

Figure 3 shows simplified block diagram of UWA OFDM system. In the transmitter, a serial bit-stream input data that is to be mapped. Hereafter, the serial data streams are converted to N-parallel data streams and then a pilot signal is inserted. OFDM modulation is conducted by using IFFT. In order to reduce the effect of ISI, cyclic prefix signal is used and ensure the orthogonality of sub carriers. After that, P/S and D/A conversion take place. In the receiver, the Doppler shift index Δ is estimated by using cyclic prefix and is compensated effectively by resampling (using a sampling rate $(1+\Delta)/T$ in the receiver different form the rate of 1/T in the transmitter) the received signal [14]. It is followed by S/P and FFT. Pilot signal is used to estimate the channel and the phase variety must be tracked in OFDM system. In time domain, the equalization is implemented.

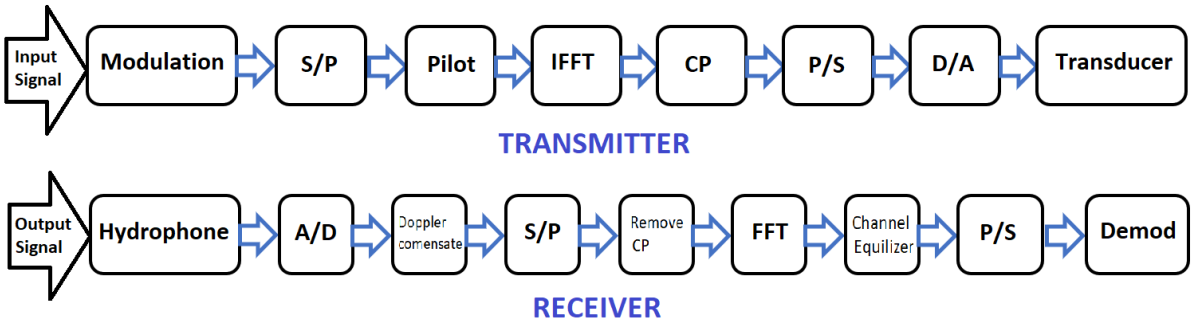

Fig. 3 Block diagram of UWA OFDM

Choice of OFDM parameters for Underwater Communication:

The choice of OFDM parameters for underwater communication is a trade-off between various competing needs. Three key requirements for the design of OFDM systems are bandwidth, bit rate and tolerable delay range. Bandwidth is the usable system bandwidth available; bit rate is the necessary error-free communication speed and tolerable delay range is the one experienced because of the multipath channel. Because of the attenuation caused by absorption which increases with frequency, useful bandwidth available for underwater communication is severely limited. Hence, low frequency communication can only be used for long-range communication. As an example, only 1 kHz bandwidth is available for 100 km range which significantly reduces the potential bit rate. We may provide greater bandwidth for short range communication and reach a high bit rate, in this case the bandwidth provided by the transducer is the main limiting factor. Another important observation to be considered regarding the acoustic bandwidth is that underwater acoustic communication is wideband communication. The useful bandwidth is often on the order of the centre frequency. Many of the current concepts of radio communication are based on narrowband communication, where the bandwidth is much smaller than that of the Centre. Consequently, the existing signal processing methods adopted for radio communication cannot be adopted for acoustic communication which results in complex requirements for signal processing. The fact that bandwidth is limited means the need for methods of modulation that are effective in bandwidth, if over such channels more than 1 b / s / Hz is to be achieved. The inverse spread of channel delay is the bandwidth of channel coherence. It shows the analysis of the frequency band that is strongly associated with the fading over. If the channel is frequency selective, it is preferable to choose narrow bandwidth for the sub-carriers. According to the Doppler spread, channel coherence time indicates the duration of the signal. The arrangement of the sub-carrier and the duration of the symbols is strongly determined by the bandwidth of coherence and the Doppler spread.

The bandwidth of channel coherence which is the opposite of the delay spread. This is a function of the band width of frequencies that strongly correlate the fading over. It is preferable to have narrower bandwidth for sub-carriers for frequency selective fading but it is required for larger Doppler spreading of wider sub-carrier bandwidth. The symbol duration and in turn the sub-carrier spacing is determined by both coherent bandwidth and Doppler spread.

The guard time should be chosen to be larger than the channel delay spread. The symbol duration should be much longer than the delay spread to minimize the SNR loss. If the symbol duration is very large, the spacing between the subcarriers is very less which increases sensitivity to frequency offset phase noise errors and also increases the peak-to-average ratio (PAPR). Implementing the signal processing thus increases complexity. Practical selection of sub-carrier spacing is a tradeoff between the channel coherence bandwidth and channel consistency time for the available bandwidth and in effect the number of sub-carriers. The number of subcarriers is determined by the required bit rate, divided by the bit rate of the subcarriers. Estimation of channels is important to improve the efficiency of the OFDM systems. Precise estimation of the channels leads to optimum selection of OFDM parameters resulting in an effective communication method.

OFDM Advantages:

OFDM has many advantages to be chosen for underwater communication scheme. The limited underwater acoustic bandwidth can be utilized efficiently by the use of OFDM. OFDM makes efficient use of the spectrum by allowing overlap between sub-carriers. Introduction of guard time with cyclic prefix greatly decreases inter-symbol interference and inter-carrier interference and hence the modulation scheme is robust against ISI and ICI. OFDM is more prone to frequency selective fading by splitting the broadband

frequency selective channel into narrowband flat fading subchannels. It is computationally effective to implement the modulation and demodulation functions using IFFT and FFT techniques. Besides the advantages of the simple OFDM system, the efficiency of the underwater channel communication scheme can be further enhanced in the following ways. By the introduction of pilot carriers appropriately, effects due to channel distortion can be corrected. Introduction of Forward Error Correction (FEC) coding and interleaving can improve the performance of the communication scheme by reducing the Bit Error Rate (BER) significantly.

THREATS AND CHALLENGES:

UWSNs are vulnerable to intimidation and malicious attacks. Attacks can be passive or active, depending on actions taken by the malicious attacker.

Passive Attacks:

The passive attacks relate to attempts by malicious nodes to interpret the essence of the activity and to acquire data transmitted in the network without interrupting the service. For example, eavesdropping, interference, confidential information leakage, impersonation, message replay and manipulation of messages. Moreover, by analyzing the traffic, observing the packet exchange, identifying communicating hosts, and determining the location, the attacker will catch the packets and then predict the nature of communication. These passive attacks are hard to detect, because passive attacks do not affect the network activity. The best solution to avoid this problem is encryption mechanisms which make it difficult for eavesdroppers to gain any information.

Active Attacks:

The active attacks attempt to modify, insert, erase or destroy the transmitted data on the network. Active attacks can intercept data, and attempt to modify or drop packets that can be executed by malicious internal or external attackers. External attacks from nodes not belonging to the network which would be easier to detect and protect. The internal attacks originate from insider nodes, and can cause serious harm. Detecting and isolating a malicious node from disrupting the network which disguised itself as a normal node is unfeasible. In addition, some internal attacks can originate from compromised nodes that actually form part of the network. Internal attacks are therefore more difficult to detect and could result in more serious damage. The only way to prevent this problem is to use security mechanisms, such as encryption, authentication and trust management. Active attacks may be classified as below [15], depending on the purpose of attacks as shown in figure 4.

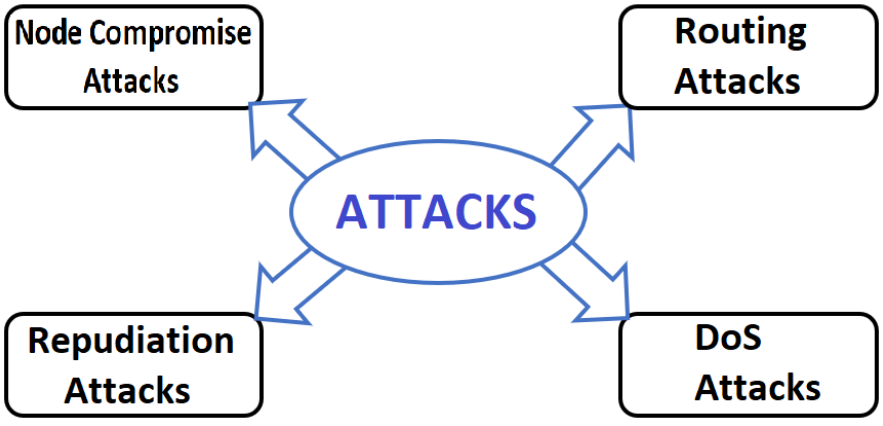

Fig. 4 Types of active attacks

Node Compromise Attacks: Underwater sensor nodes can be deployed in some special fields of application in unattended and even worse hostile regions of the sea. Through addition, the network may consist of tens or hundreds of nodes deployed in large scales, meaning that it cannot guarantee the safety of all nodes. An attacker may catch, crack and compromise nodes to read or alter memory data. Even worse, the compromised nodes can be injected into the network as a legitimate node for monitoring or disturbing, resulting in more serious damage.

Repudiation Attacks: Malicious nodes deny having any role in specific action or communication with other nodes in repudiation attacks. Refers to denial of having participated in all or part of the communication by a node involved in a communication, irrespective of whether that communication is malicious or not.

Routing Attacks: Routing attacks may trigger packets that cannot be transmitted to the destination node, which may even be worth disrupting the network activity. Such kinds of attacks are built on the routing protocols, for example table routing overload, table routing poisoning, packet duplication, and rushing attack. Attackers can collect packets and analyze or even drop packets at their will through these malicious behaviors. Cryptographic approaches are the routing attacks are also used to shield. Using encryption, however, not only increases the size of contact messages but also creates more energy consumption due to the high complexity of computations.

DoS Attacks: DoS is a kind of aggressive attack that tries to make the legitimate nodes inaccessible for resources. The attacker has tried to block legitimate nodes from accessing the network's services. DoS attacks can be carried out in a variety of different directions but still causing the same problems.

DoS attacks are more damaging and harder to detect between these active attacks [16]. The approaches to the attacks should be comprehended to avoid UWSNs from DoS attacks. DoS attacks can be initiated in various ways and at any layer of the protocol stack. Malicious attackers can cause severe damages with very low cost, impersonate as a legitimate node to deceive neighbor nodes, or impose especially high-power cost tasks Legitimate nodes to shorten the lifetime of nodes [17].

SECURITY REQUIREMENTS:

The security requirements of UWSNs as a branch of WSNs are similar to terrestrial WSNs [18]. But there are also some special security requirements due to the particularities and constraints of the UWSNs as shown in figure 5.

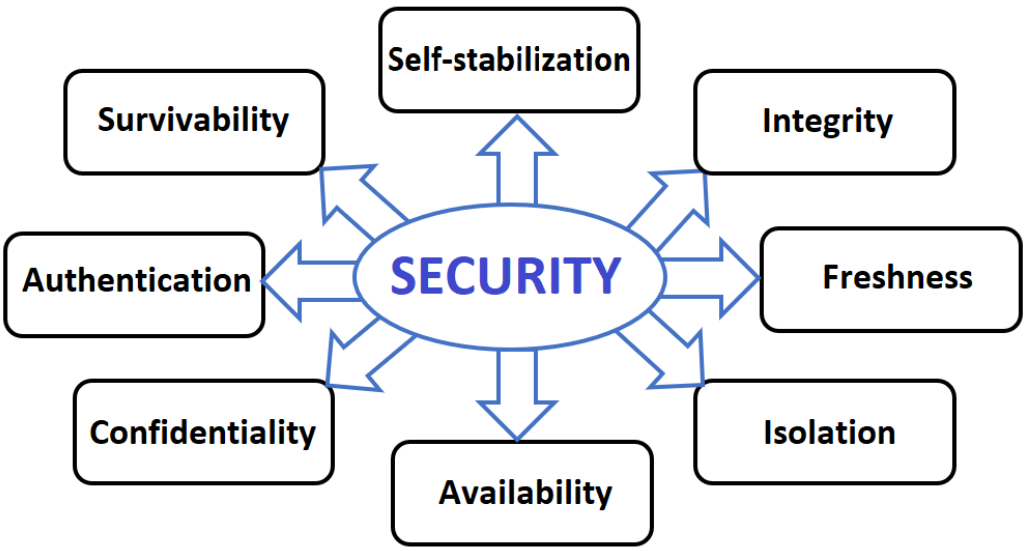

Fig. 5 Security requirement.

Confidentiality:

It is about preventing unauthorized nodes from understanding sensitive data contents (e.g., security credentials and secret keys). Confidentiality is not limited to the survivability of knowledge about users (strategic or tactical military information, for example), but also for MAC survivability, routing information, etc. Those sensitive data should be prevented by malicious attacker from reading or manipulating. Confidentiality can be accomplished by applying technique of low-power efficient encryption that is ideal for UWSNs. The Cipher Text Theft (CTS) technique [19] is a characteristic lightweight encryption technique used in UWSNs.

Authentication:

As discussed above, the acoustic channel is also open, and the malicious attacker can easily catch packets and change the content without encryption techniques. Receiving node therefore needs to classify the data base to detect malicious attacks. Nodes need permission to access and share channels, resources, programs, and data on the network. Mechanism for detecting intrusions and maintaining trust identify suspicious behaviours to disable network malicious nodes. These protocols ensure that the approved nodes are able to operate in the network.

Integrity:

Data integrity is to ensure that the data received is not changed, deleted or compromised by unauthorized nodes, either by radio failure or malicious attack during transition. That is most relevant in such circumstances as military operations and controls of equipment where these modifications may cause serious harm. WSNs and UWSNs have commonly implemented the Message Authentication Code (MAC) [20] for data authentication, which has good scalability, low latency, reliability, adaptability and ease of implementation.

Availability:

Availability is to ensure the network needs to be sufficiently stable. Even if other nodes failed or the network was targeted, it could still provide services. Proper operational flexibility and self-adaptive techniques will provide UWSN availability.

Isolation:

Isolation is to ensure nodes are capable of identifying abnormal activities and removing malicious nodes. In addition, routing protocols, MAC protocols, should be immune to malicious attacks. Appropriate data protection and lightweight algorithms to cryptography can be used to separate malicious nodes.

Freshness:

Freshness is to ensure that the data received is fresh, and that legacy data is not retransmitted. Updates to routing should be made available in real time. The delay in updating messages may indicate the incorrect state of network and result in massive knowledge loss.

Self-stabilization:

Self-stabilization is to ensure that nodes can recover independently from attacks in real time without any intervention. If node is self-stabilizing to malicious attacks, even if the attacker remained in the network, it may recover to normal state by itself.

Survivability:

It is the system's ability to perform on its mission in a timely manner, in the presence of disaster, malfunction, intrusion or malicious attack. This is to ensure that the network can restore and maintain essential services during and after malicious attacks, even though part of the network was destroyed.

SECURITY ISSUES OF UWSNs:

UWSNs are vulnerable to diverse threats and attacks. A collection of mechanisms and security technologies to protect UWSNs from attacks must be proposed to attain the objectives of the security requirements. The security concerns of UWSNs are logically divided into separate components according to the OSI network. The security issues mainly include: key management, intrusion detection, trust management, secure localization, secure synchronization, and routing security as shown in figure 6.

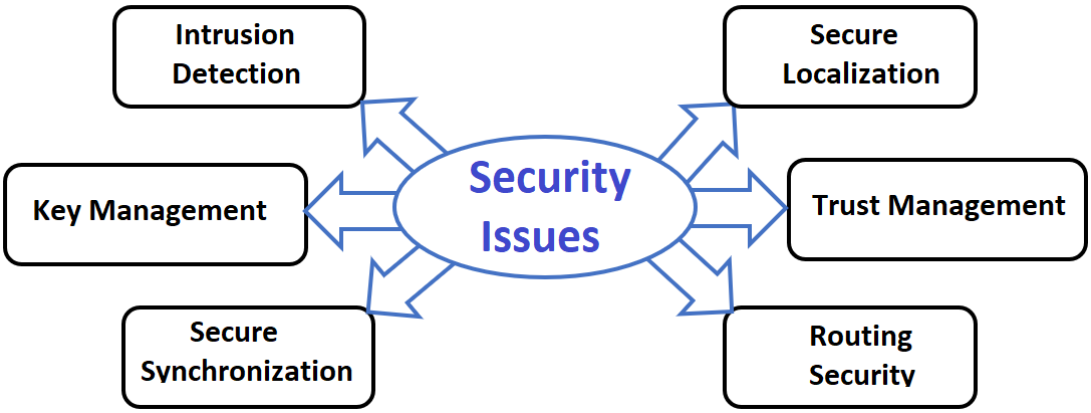

Fig. 6 Different security issues of UWSN

Key Management:

Cryptography and key management main purposes are confidentiality, security, honesty, and non-repudiation. Cryptography allows the storage or delivery of sensitive information in unsafe networks such as the underwater acoustic channel, so that it cannot be read or modified by unauthorized users. Unfortunately, some problems suffer from the existing cryptography and key management mechanisms, including expansion of cipher texts and computational complexity. Message padding and codes increase the length of the message after cryptography and cause more energy consumption when transmitting and

computing [21]. Digital signatures are usually used to authenticate messages. An authenticated message is attached to a digest, which will enable expansion and overhead communication [22].

Trust Management:

As an important complement to cryptographic-based security defense, the trust management mechanism has significant benefits in detecting intrusions. The research on trust management mechanisms in UWSNs faces more challenges because of the peculiarities and constraints of UWSNs [23]. Classification of existing trust management mechanisms can be into three categories: centralized scheme, distributed scheme, and hierarchical scheme. A root node or a base station provides trust protection for each sensor node in centralized scheme. The centralized systems are inadequate for UWSNs, since a costly burden is the energy consumption of confidence values sharing between the sensor nodes and base station. Each node needs to calculate and maintain the trust values of the entire network in distributed scheme. But for UWSNs it is impossible, because underwater sensor nodes in hardware resources are extremely limited. Therefore, the distributed systems are also unsuitable for UWSNs. As discussed above, it is obvious that the UWSNs are not suitable for either pure centralized or pure distributed schemes. The calculation and transmission of confidence value is implemented in hierarchical schemes in a hierarchical manner. The confidence values are passed and fused from lower to upper layer. The hierarchical schemes are therefore more suitable for cluster-based topology that has been widely used in UWSNs. The sink node must be able to authenticate itself in order to transmit control information and retrieve the readings from the underwater sensor nodes.

Localization Security:

Location estimation is a crucial component in the application of source detection and tracking. During the localization phase, the underwater sensor nodes get the location information and speed of mobile nodes, which would be used to select the best relay node for transmitting data. The sink node can't determine where the obtained data originates without the location information. Localization protocols proposed for WSNs cannot function in underwater applications because of the underwater channel characteristics [24]. Some attacks specific to the localization, e.g. Sybil attack, black hole attack, and wormhole attack can cause great damage through the use or alteration of the position information. Even in the presence of Sybil and wormhole attacks, the secure localization scheme should be able to determine the location of sensors and the scheme should be able to node mobility in UWSNs.

Routing Security:

The routing security consists of basic transports and security mechanisms for connectivity applied to routing protocols as well as to individual nodes. In addition, nodes must exchange neighboring information to build network topology for the application of one of the routing protocols (Proactive, Reactive and Hybrid). Routing security involves two aspects: secure routing and secure data forwarding. Nodes are expected to cooperate in secure routing in order to exchange appropriate routing information, thus keeping the network connected efficiently, therefore data packets must be shielded from being manipulated, dropped and altered by any unauthorized party during secure data transmission.

Intrusion Detection:

Mechanisms for intrusion detection are the detection, recognition and exclusion of internal or external intruders from the network. However, mechanisms for detecting intrusion usually work after the malicious attacks have taken effect and have been discovered. First time that attacks have taken effect, it is hard to detect malicious intruders. So, mechanisms for real-time detection need to be investigated and improved. Alternatively, systems may be used tolerance to intrusion protect networks while allowing malicious intruders to exist, which is regarded as an effective security mechanism. In addition, algorithms technologies and intrusion detection systems (IDS) were proposed to further improve the security of UWSNs. Hierarchical IDS is suitable for multilayered UWSNs, in which cluster head nodes perform the IDS task and act as checkpoints, such as wired network routers. Among these types of IDS, the hierarchical IDS is appropriate for cluster structure-based UWSNs.

Synchronization Security:

Synchronization is essential in many underwater applications and scheduling MAC protocols. The proposed synchronization security protocols are unsuitable for UWSNs. Additionally, precise time synchronization in underwater conditions is especially difficult to achieve. Although it is critical in the UWSNs issues, none of the existing time synchronization schemes [25- 26] took security in consideration. Proper cryptographic methods can be used to combat time synchronization attacks, e.g. masquerade, replay, and manipulation attacks. However, the countermeasures suggested [27-29] against delay attacks for WSNs do not extend to UWSNs

CONCLUSION:

In this study, we over viewed the major challenges for efficient communications within networks of underwater acoustic sensors. We outlined the underwater channel peculiarities, with specific regard to networking solutions for monitoring ocean environment applications. Then we talked about OFDM that has been used in UWA communication channel. OFDM system is more efficient for high rate UWA communication not only at short range, but also at medium range. UWSNs are vulnerable to a variety of security threats and malicious attacks, which seriously disrupt the network's communication and cooperation. The security specifications of UWSNs are added to prevent these attacks. Ultimately, it addresses several different information systems and protection schemes. Because of the peculiarities and constraints, it is not easy to secure UWANs, as discussed. In addition, applications may have special security specifications, and unnecessary protection schemes would be a heavy burden on energy consumption. Hence, how these features can be taken into account in the design of the protection scheme is also an important subject in future research.

REFERENCES

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

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

[3] J. G. Proakis, E. M. Sozer, J. A. Rice, and M. Stojanovic, "Shallow water acoustic networks," IEEE Communications Magazine, pp. 114–119, Nov. 2001.

[4] I. F. Akyildiz, D. Pompili, and T.Melodia, "Underwater acoustic sensor networks: research challenges," Ad Hoc Networks, vol. 3, no. 3, pp. 257–279, 2005.

[5] Ian F. Akyildiz, Dario Pompili, and Tommaso Melodia. 2004. Challenges for efficient communication in underwater acoustic sensor networks. SIGBED Rev. 1, 2 (July 2004), 3–8. DOI: https://doi.org/10.1145/1121776.1121779

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

[7] 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, ACM, September 2006.

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

[9] D. H. Cato, "Ocean ambient noise: Its measurement and its significance tomarine animals," in Proceedings of the Conference on Underwater Noise Measurement, Impact and Mitigation, pp. 1–9, Institute of Acoustics, Southampton, UK, 2008.

[10] N.-S. N. Ismail, L. A. Hussein, and S. H. S. Ariffin, "Analyzing the performance of acoustic channel in underwater wireless sensor network (UWSN)," in Proceedings of the Asia Modelling Symposium 2010: 4th International Conference onMathematical Modelling and Computer Simulation, AMS2010, pp. 550–555, Malaysia, May 2010.

[11] S. Basagni, C. Petrioli, R. Petroccia, andM. Stojanovic, "Optimizing network performance through packet fragmentation in multi-hop underwater communications," in Proceedings of the OCEANS'10 IEEE Sydney, OCEANSSYD 2010, pp. 1–7, Australia, May 2010.

[12] K. A. Perrine, K. F. Nieman, T. L. Henderson, K. H. Lent, T. J. Brudner, and B. L. Evans, "Doppler estimation and correction for shallow underwater acoustic communications," in Proceedings of the 44th Asilomar Conference on Signals, Systems and Computers, Asilomar 2010, pp. 746–750,USA,November 2010.

[13] X. Zhang, X. Han, J. Yin, and X. Sheng, "Study on Doppler effects estimate in underwater acoustic communication," in Proceedings of the ICA 2013 Montreal, pp. 070062-070062, Montreal, Canada, 2013.

[14] Shanif B, Neasham J, Hinton 0 R, Adams A E. A computationally efficient Doppler compensation system for underwater acoustic communications. IEEE Journal of Oceanic Engineering, 2000, system for a 10km range UWA communication 25(l):52-60

[15] Wood A D, Stankovic J A. Denial of service in sensor networks[J]. Computer, 2002, 35(10): 54-62.

[16] Raymond D R, Midkiff S F. Denial-of-service in wireless sensor networks: Attacks and defences[J]. IEEE Pervasive Computing, 2008 (1): 74-81.

[17] Hu Y C. A defence against wormhole attacks in wireless networks[J]. IEEE INFOCOM 2003, Mar., 2003.

[18] Lopez J, Roman R, Alcaraz C. Analysis of security threats, requirements, technologies and standards in wireless sensor networks[M]//Foundations of Security Analysis and Design V. Springer, Berlin, Heidelberg, 2009: 289-338.

[19] Law Y W, Doumen J, Hartel P. Survey and benchmark of block ciphers for wireless sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2006, 2(1): 65-93.

[20] Bellare M, Canetti R, Krawczyk H. Keying hash functions for message authentication[C]//Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1996: 1-15.

[21] Dini G, Lo Duca A. A secure communication suite for underwater acoustic sensor networks[J]. Sensors, 2012, 12(11): 15133-15158.

[22] Jiang S. Wireless Networking Principles: From Terrestrial to Underwater Acoustic[M]. Springer Singapore, 2018.

[23] Goyal N, Dave M, Verma A K. Trust model for cluster head validation in underwater wireless sensor networks[J]. Underwater Technology, 2017, 34(3).
[24] Han G, Liu L, Jiang J, et al. A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks[J]. Sensors, 2016, 16(2): 229.
[25]] Liu J, Wang Z, Zuba M, et al. DA-Sync: A Doppler-assisted time-synchronization scheme for mobile underwater sensor networks[J]. IEEE Transactions on Mobile Computing, 2014, 13(3): 582-595.
[26] Liu J, Wang Z, Peng Z, et al. TSMU: A time synchronization scheme for mobile underwater sensor networks[C]//Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE. IEEE, 2011: 1-6.
[27] Song H, Zhu S, Cao G. Attack-resilient time synchronization for wireless sensor networks[J]. Ad Hoc Networks, 2007, 5(1): 112-125.
[28] Boukerche A, Turgut D. Secure time synchronization protocols for wireless sensor networks[J]. IEEE Wireless Communications, 2007, 14(5).
[29] Du X, Guizani M, Xiao Y, et al. Secure and efficient time synchronization in heterogeneous sensor networks[J]. IEEE transactions on vehicular technology, 2008, 57(4): 2387-2394

THE END