INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SPECIAL ISSUE FOR INTERNATIONAL LEVEL CONFERENCE "ADVANCES IN SCIENCE, TECHNOLOGY & MANAGEMENT" (IC-ASTM)

SECURING UNDERWATER WIRELESS COMMUNICATION NETWORKS BY ACOUSTIC CHANNELS

PROF. PRIYA A. TAYADE, PROF. S. V. NAROTE

Assistant Professor, *Department of Computer Science and Engineering*, Amravati University, Maharashtra State, India.

Accepted Date: 05/09/2017; Published Date: 10/10/2017

Abstract: In last several years, underwater communication network (UWCN) has found an increasing use in a widespread range of applications, such as coastal surveillance systems, environmental research, autonomous underwater vehicle (AUV) operation, oil-rig maintenance, collection of data for water monitoring, linking submarines to land, to name a few. Underwater wireless communication networks are particularly vulnerable to malicious attacks due to the high bit error rates, large and variable propagation delays, and low bandwidth of acoustic channels. The unique characteristics of the underwater acoustic communication channel and the differences between underwater sensor networks and their ground-based counterparts require the development of efficient and reliable security mechanisms. In this seminar, a complete survey of security for UWCNs is presented, and the research challenge for secure communication in this environment is outlined. The research of Underwater Acoustic Networks (UANs) is attracting attention due to their important underwater applications for military and commercial purposes. Underwater wireless communication networks (UWCNs) consist of sensors and autonomous underwater vehicles (AUVs) that interact, coordinate and share information with each other to carry out sensing and monitoring functions.

Keywords: Underwater wireless communication networks, Autonomous underwater vehicle, sensor nodes, hybrid communication, underwater acoustic network.

Corresponding Author: PROF. PRIYA A. TAYADE

Co Author: - PROF. S. V. NAROTE

Access Online On:

www.ijpret.com

How to Cite This Article:

Priya A. Tayade, IJPRET, 2017; Volume 6 (2): 288-293

PAPER-QR CODE

INTRODUCTION

The aquatic environment is particularly unreliable to malicious attacks due to the high bit error rates, large and variable. propagation delays, and low bandwidth of acoustic channels. Wireless is a term used to describe the telecommunication in which the electromagnetic waves carry the signal over part or all of the communication path. The signals that are used to carry digital information through an underwater channel are not radio signals as electromagnetic waves propagate over short distances. Instead acoustic waves are used which can propagate over long distances.

Acoustic communications is defined as communication methods from one point to another by using acoustic signals. Acoustic signal is the only physical feasible tool that works in underwater environment. Compared with it electromagnetic wave can only travel in water with short distance due to the high attenuation and absorption effect in underwater environment. There are some investigations about utilizing optical signal for underwater applications. However, they find out that optical signal can only pass through limited range in very clean water environment (deep water, for example). Underwater Acoustic Networks, including but not limited to, Underwater Acoustic Sensor Networks (UASNs)and Autonomous Underwater Vehicle Networks (AUVNs), are defined as networks composed of more than two nodes, using acoustic signals to communicate, for the purpose of underwater applications.

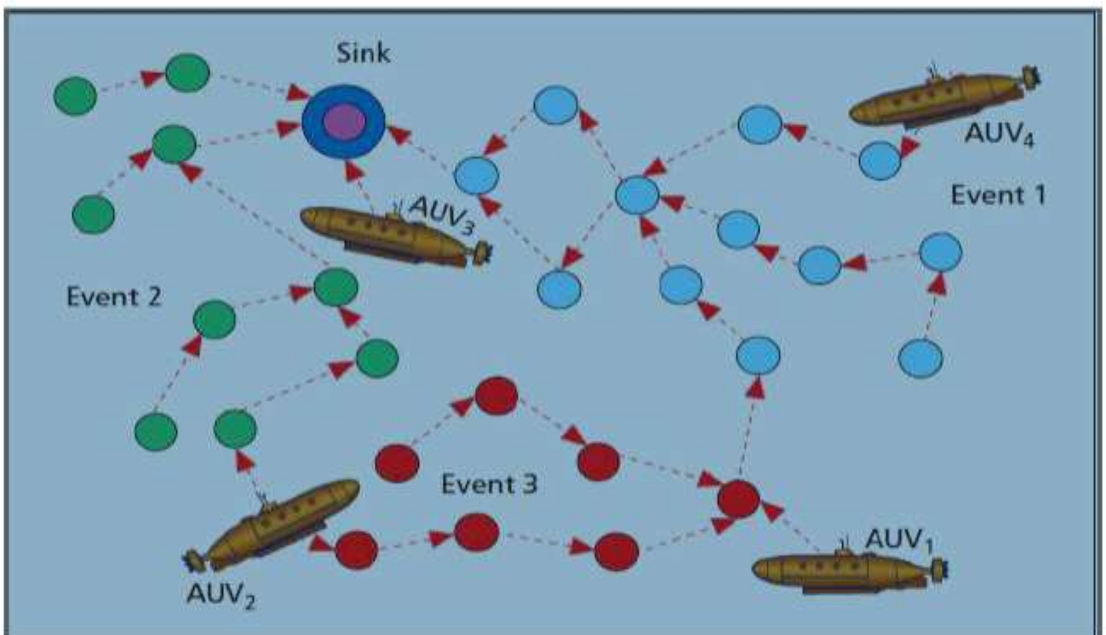

Fig.1 Underwater sensor network with AUV

2. NECESSITY OF UNDERWATER WIRELESS COMMUNICATION

Wired underwater is not feasible in all situations as shown below-:

- Temporary experiments
- Breaking of wires
- Significant cost of deployment
- Experiment over long distances.

To cope up with above situations, we require underwater wireless communication. As wireless communication technology today has become part of our daily life, the idea of wireless undersea communications may still seem far-fetched. However, research has been active for over a decade on designing the methods for wireless information transmission underwater. Human knowledge and understanding of the world's oceans, which constitute the major part of our planet, rests on our ability to collect information from remote undersea locations.

3. ATTACKS ON UWCNS

A jamming attack consists of interfering with the physical channel by putting up carriers on the frequencies neighbor nodes use to communicate. Since underwater acoustic frequency bands are narrow, UWCNs are vulnerable to narrowband jamming.

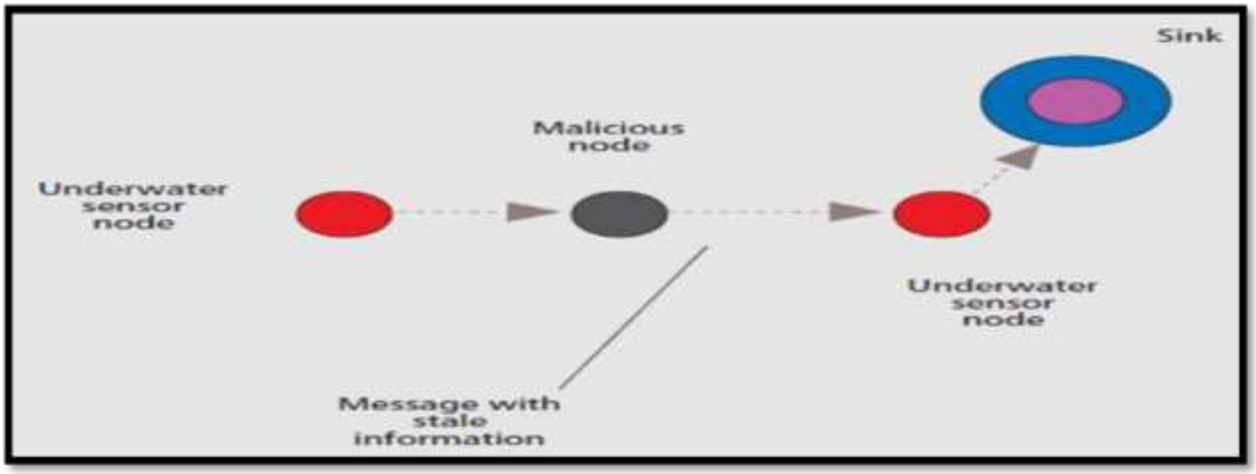

Fig 2: Jamming Attack

Localization is affected by the replay attack when the attacker jams the communication between a sender and a receiver, and later replays the same message with stale information posing as the sender

A. Wormhole Attack:

A wormhole is an out-of-band connection created by the adversary between two physical locations in a network with lower delay and higher bandwidth than ordinary connections. This connection uses fast radio (above the sea surface) or wired links to significantly decrease the propagation delay.

B. Sybil Attack:

An attacker with multiple identities can pretend to be in many places at once. Geographic routing protocols are also misled because an adversary with multiple identities can claim to be in multiple places at once. Authentication and position verification are methods against this attack, although position verification in UWCNs is problematic due to mobility.

C. Sinkhole Attack:

In a sinkhole attack, a malicious node attempts to attract traffic from a particular area toward it; for example, the malicious node can announce a high-quality route. Geographic routing and authentication of nodes exchanging routing information are possible defenses against this attack, but geographic routing is still an open research topic in UWCNs.

D. Hello Flood Attack:

A node receiving a HELLO packet from a malicious node may interpret that the adversary is a neighbor; this assumption is false if the adversary uses high power for transmission. Bidirectional link verification can help protect against this attack, although it is not accurate due to node mobility and the high propagation delays of UWCNs. Authentication is also a possible defense.

4. ACOUSTIC COMMUNICATION

Multicarrier modulation: The idea of multicarrier modulation is to divide the available bandwidth into a large number of overlapping sub bands, so that the waveform duration for the symbol at each sub band is long compared to the multipath spread of the channel Consequently, inter-symbol interference may be neglected in each sub band, greatly simplifying the receiver complexity of channel equalization. Precisely due to this advantage, multicarrier modulation in the form of orthogonal frequency division multiplexing (OFDM) has prevailed in recent broadband wireless radio applications.

Multi-input multi-output techniques: A wireless system that employs multiple transmitters and multiple receivers is referred to as a multiple-input multiple-output (MIMO) system Hence, MIMO modulation is a promising technology to offer yet another fundamental advance on high data rate underwater acoustic communication. MIMO has been applied in both single carrier transmission and multicarrier transmission.

Understanding the first principles of each physical wave used in UWSN wireless communication is critically important. In this section we layout the fundamental physical properties and critical issues for each of the acoustic and optical wave propagations in underwater environments. We discuss each physical carrier's advantages and disadvantages towards efficient underwater wireless communication.

Acoustic Waves

Among the types of waves, acoustic waves are used as the primary carrier for underwater wireless communication systems due to the relatively low absorption in underwater environments. We start the discussion with the physical fundamentals and the implications of using acoustic waves as the wireless communication carrier in underwater environments.

An acoustic wave has a number of propagation characteristics that are unique from other waves, one of which is highlighted below:

Propagation velocity:

The extremely slow propagation speed of sound through water is an important factor that differentiates it from electromagnetic propagation. A typical speed of sound in water near the ocean surface is about 1520 m/s, which is more than 4 times faster than the speed of sound in air, but five orders of magnitude smaller than the speed of light. The speed of sound in water increases with increasing water temperature. As depth increases, the pressure of water has the largest effect on the speed of sound.

5. SECURITY REQUIREMENTS

In UWCNs the following security requirements should be considered:

1. Authentication: Authentication is the proof that the data was sent by a legitimate sender. It is essential in military and safety-critical applications of UWCNs. Authentication and key establishment are strongly related because once two or more entities verify each other's authenticity, they can establish one or more secret keys over the open acoustic channel to exchange information securely; conversely, an already established key can be used to perform authentication.

2. Confidentiality: Confidentiality means that information is not accessible to unauthorized third parties. Therefore, confidentiality in critical applications such as maritime surveillance should be guaranteed.

3. Integrity: It ensures that information has not been altered by any adversary. Many underwater sensor applications for environmental preservation, such as water quality monitoring, rely on the integrity of information.

4. Availability: The data should be available when needed by an authorized user. Lack of availability due to denial-of-service attacks would especially affect time-critical aquatic exploration applications such as prediction of seaquakes.

6. RESEARCH CHALLENGES

There is various security issues in UWCNs related to routing, localization, secure time synchronization are described below:

1) Secure time synchronization:

In underwater applications time synchronization is very important like coordinated sensing tasks. Scheduling algorithms such as time division multiple access (TDMA) needed lot of time to adjust their wake-sleep schedules between nodes for power saving but it's very difficult to achieve lot of time synchronization in UWCNs due to its characteristics. This is the reason we cannot use the time synchronization mechanism proposed for ground based sensor networks. New mechanisms have been proposed. Tri-Message is a time synchronization protocol designed for high-latency networks with a synchronization precision that increases with distance. A multilateration algorithm is proposed in for localization and synchronization in 3D underwater caustic sensor networks.

2) Secure Localization:

Localization is a very important issue for data tagging. Sensor tasks such as reporting the occurrence of an event or monitoring require localization information. Localization can also help in making routing decisions. Unlike in the terrestrial positioning, the global positioning system (GPS) cannot work efficiently underwater. The limited bandwidth, the severely impaired channel and the cost of underwater equipment all makes the localization problem very challenging. Most current localization schemes are not well suitable for deep underwater environment.

Localization schemes can be classified into:

a. Range-Based Schemes (using range and/or bearing information): The location of nodes in the network is estimated through precise distance or angle measurements.

b. Range-Free Schemes (Not Using Range or Bearing Information): They have been designed as simple schemes to compute only coarse position estimates. A range-free scheme estimates the location of a sensor within a certain area.

3)Secure Routing:

Routing is essential for packet delivery in UWCNs. For example, the Distributed Underwater Clustering Scheme (DUCS) does not use flooding and minimizes the proactive routing message exchange. Underwater Acoustic Sensor Networks (UASNs) have drawn great attention for their potential value in ocean monitoring and offshore exploration. In order to make the underwater application possible, the unique characteristics of underwater acoustic channels and continuous node movement inspired the emergence of routing protocols for underwater environment.

7. APPLICATIONS

- Future applications could enhance myriad industries, ranging from the offshore oil industry to aquaculture to fishing industries, pollution control, climate recording, ocean monitoring (for prediction of natural disturbances) and detection of objects on the ocean floor are other areas that could benefit from enhanced underwater communications.
- Environmental monitoring to gathering of oceanographic data
- Marine archaeology
- Search and rescue missions
- Defense

8. ADVANTAGES AND DISADVANTAGES

Advantages

- It avoids data spoofing
- It avoids privacy leakage
- Minimize communication and computational cost.
- Maximizes the battery power by preserving the power of underwater sensors

Disadvantages

- Battery power is limited and usually batteries cannot be recharged also because solar energy cannot be exploited .
- The available bandwidth is severely limited.
- Channel characteristics including long and variable propagation delays
- Multipath and fading problems.
- High bit error rate.

.

8. CONCLUSIONS

This paper gives the overall view of the necessity of underwater wireless communication and its applications. Despite much development in this area of the underwater wireless communication, there is still an immense scope so more research as major part of the ocean bottom yet remains unexploded. Underwater Sensor Networks is a very recent technology that tries to follow the same steps than terrestrial wireless networks in a very different and challenging network environment. There is an increasing interest in USWN technologies and their potential applications. The main research challenges related to secure time synchronization, localization, and routing have also been surveyed. The research issues remain wide open for future investigation, and find the best technique is range free distributed positioning scheme. However, the complexity and cost of the system are increased.

REFERENCES

1. M. Chitre, S. Shahabudeen, and M. Stojanovic, *"Underwater Acoustic Communications Networking: Recent Advances and Future Challenges,"*Marine Technology Society Journal vol.Spring 2008, pp. 103- 116, 2008.
2. Weichao Wang, Jiejun Kong, “Visualisation of wormholes in underwater sensor networks: a distributed approach”, Int. J. Security and Networks, Vol. 3, No. 1, 2008.
3. “Securing Underwater Wireless Communication Networks”, Electrical and Electronics Engg. Seminar Report 2013.
4. Ashvini P. and Sivasankaran V., “Securing Underwater Wireless Communication Networks-Literature Review”, ARPN Journal of Engineering and Applied Sciences .©2006-2015 Asian Research Publishing Network (ARPN). All rights reserved.
5. Guangjie Han,1,2Jinfang Jiang,1,2 Lei Shu,3 Yongjun Xu,4 and Feng Wang5Sensors (Basel). 2012; 12(2): 2026–2061. Published online 2012 Feb 13. doi: 10.3390/s120202026.
6. Samedha S. Naik1, Manisha J. Nene2, “REALIZATION OF 3D UNDERWATER WIRELESSSENSOR NETWORKS AND INFLUENCE OF OCEANPARAMETERS ON NODE LOCATION ESTIMATION”, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 2, April 2012.