On Security and Energy Efficiency in Underwater Wireless Sensor Networks for Maritime Border Surveillance

Seungmo Kim*
*seungmokim@georgiasouthern.edu
Department of Electrical and Computer Engineering
Georgia Southern University
Statesboro, GA, USA

***Abstract*—Underwater wireless sensor networks (UWSNs) based on acoustic communications attract interest as an enabling technology of maritime border surveillance. However, due to differences in environments, many of the techniques used in typical terrestrial wireless communications are not directly applicable to UWSNs. Of the challenges, designing a secured and energy-efficient UWSN takes the greatest significance for application to maritime surveillance applications. To provide an overview on the UWSN technology, this paper (i) characterizes key technical challenges that are drawn in UWSNs and (ii) discusses methodologies to improve security and energy efficiency of an UWSN.**

***Index Terms*—Underwater acoustic communications; UWSN; Security; Energy efficiency**

I. Introduction

Underwater wireless sensor networks (UWSNs) contain several components such as vehicles and sensors that are deployed in a given geographic area to perform collaborative monitoring and data collection tasks. Today, the UWSN has become a key wireless communication technology that can be used for a wide range of homeland security applications including tactical surveillance, offshore exploration, monitoring of subsea machinery such as oil-rigs and pipelines.

A. Challenges

Nonetheless, it is still a daunting task to establish a stable UWSN due to several key challenges. Focusing on maritime border surveillance applications, we identify the following two challenges particularly important to revolve.

1) Challenges in Security: First, *time synchronization* is important in several underwater applications resembling coordinated sensing tasks. Also, programming algorithms resembling time division multiple access (TDMA) need precise temporal order between nodes to regulate their sleep-wake up schedules for power saving. Achieving precise time synchronization is particularly tough in underwater environments because of the characteristics of UWSNs.

Second, *localization* could be a vital issue for detection and sharing the sensed knowledge. Nevertheless, the localization techniques built for ground-based wireless networks cannot be directly be applied to the underwater underwater environment because of the aforementioned unique challenges. Hence, more concern should be given to the architecture of underwater wireless networks.

2) Challenges in Energy Efficiency: With UWSN protocol designs, saving energy is a major concern, especially for long-term aquatic monitoring and sensing applications and due to its node mobility, most of the energy-efficient protocols designed for terrestrial wireless networking are not feasible [5].

B. Contribution of This Paper

As a survey, this paper describes the present-day techniques to address the challenges. We provide an extensive investigation on the system model–*i.e.*, path loss, noise, multipath, and Doppler spread–in order to draw accurate analyses subsequently. Accounting the system model, we study the methodologies to improve *security* and *energy efficiency*–the two aspects that this paper identifies as the key challenges in operation of maritime border applications.

II. System Model

The key rationale that we put a particular significance on an accurate characterization of a UWSN system model is as follows. UWSN and terrestrial wireless systems share common properties but they have critical differences, which is attributed to the communication medium.

It is less efficient for UWSNs to use radio frequency (RF) signals since they have an enormous attenuation in the subaquatic medium. Therefore, acoustic signals are more commonly used in underwater communications scenarios [1].

Acoustic communication regarding underwater environment is a complex phenomenon because a lot of environmental factors affect acoustic communication. These factors vary including long propagation delays, environmental noise, path loss, Doppler spread, and multipath effect.

A. Path Loss

When sound propagates from underwater environment then some of its strength converts into heat. Sound wave propagation energy loss can be categorized into three main categories [2]:

1) *Geometric Spreading Loss:* When source generates acoustic signal it propagates away from the source in the form of wave fronts. This loss is independent of frequency, while only depends on the distance.
2) *Attenuation:* Within acoustic communication, the most common attenuation appears as conversion into heat.

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-853-2

The level of attenuation is directly proportional to frequency and distance.

3) *Scattering Loss:* This type of loss occurs at the surface of the water. Surface roughness is usually generated by the wind, which in turn changes the pattern of scattering. Scattering at the surface of the water causes power losses of acoustic signals.

B. Noise

Types of underwater noise are two-fold [2]. First, noise can generated by *humans* while operating various activities from use of underwater machines to shipping and fishery. Second, *ambient noise* is generated by a combination of different sources that are often impossible to identify [3]. Underlying noise is considered as thermal noise in the absence of all other sources of noise, including self-noise. Thermal noise is directly proportional to the frequency which is used for acoustic communication.

C. Multipath

In terrestrial wireless communications, a multipath effect is well known to cause delay spread in a signal, which in turn cause an inter-symbol interference. In underwater acoustic communications, number of propagation paths, propagation delays, and its strength are determined by the acoustic channel impulse response that is determined by the geometry. For instance, in deep oceans, refraction of sound occurs because of variable sound speed that cases of multipath effect in acoustic channel. On the other hand, sound propagation in shallow water is influenced by surface reflections while deep water propagation is affected by bottom reflection that becomes cause of large and variable communication delay in acoustic communication.

D. Doppler Spread

In underwater environments, just as in terrestrial wireless communications scenarios, there also are relative spatial movement among a transmitter, a received, and obstacles in the middle of a communications path, which causes Doppler shift. The subsequent impact is the same to be the frequency offset.

III. Security and Energy Efficiency in UWSN

A. Security

We identify the key attack types and understand them in UWSN's perspectives as follows.

1) Jamming: A jamming attack is a type of denial of service (DoS) attack, which prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on. UWSNs area unit prone to narrowband electronic jamming due to the narrowband nature of acoustic communications.

In terrestrial networks, when a jamming is detected, the sensors are quickly able to report the intrusion to other nodes in order to re-route the packets around the impacted area. However, it is not trivial to apply this resolution to UWSNs mainly due to 'sparse deployment' of nodes in underwater scenarios. In other words, there usually are not enough sensors to provide a detour and to re-route traffic around the jammed area. Another resolution projected for ground-based detector networks against electronic countermeasures is to use various technologies for communication resembling in fared or optical. However, this resolution can't be applied either, since optical and infrared waves square measure severely attenuated below water.

2) Wormhole Attack: A wormhole attack is known to severely destroy the performance of an ad-hoc network [4]. In a wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication.

One methodology for detection of a wormhole attacker in terrestrial networks is based on estimation of the physical distance between two nodes as the key indicator of the "neighborship." However, the correct estimation of a distance depends on precise localization and tight clock synchronization. In underwater communications, both of them become extremely challenging.

3) Sybil Attack: In a sybil attack, a node in the network operates multiple identities actively at the same time and undermines the authority/power in reputation systems. The main aim of this attack is to gain the majority of influence in the network to carry out illegal (with respect to rules and laws set in the network) actions in the system. To outside observers, these multiple fake identities appear to be real unique identities.

Again, designing a countermeasure against a sybil attack in an UWSN is challenging because of the difficulty in precise localization of an underwater node. Specifically, authentication and position verification are efficient countermeasures against a sybil attack; yet the accurate position verification becomes difficult in an UWSN due to challenges in communications introduced in Section II.

B. Energy Efficiency

Since most of the underwater sensors operate on battery powers, it is essential for maritime surveillance to design an UWSN that is energy-efficient.

One popular method that can be applied to UWSN is packet size optimization. Again, selection of a packet size becomes more challenging in an UWSN due to wider variations of environmental factors. Moreover, due to the movement of sensor nodes under the influence of ocean currents, collection of information among a wide enough network also becomes an issue. This 'myopic' sight on a network hinders a faster dissemination of knowledge on 'link costs' over an entire network, which in turn causes a higher delay in routing.

IV. Conclusions

Today, UWSN has garnered a staggering amount of attention in the research society for the homeland security. How-

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-853-2

ever, when compared to terrestrial wireless sensor networks, the UWSN presents one with an intricate complexity. This study identified *security* and *energy efficiency* as the major factors to resolve in design of an UWSN. Then, it went on discussing the particular reasons that the UWSN makes it more difficult to address the two goals. This work can form the basis for further research in designing novel algorithms for managing a large number of nodes in an UWSN. It will further show a significant contribution to securing the nation's land/maritime borders.

REFERENCES

[1] S. Jiang, "On securing underwater acoustic networks: a survey," *IEEE Commun. Surveys Tut.*, vol. 21, iss. 1, 2019.

[2] P. Amoli, "An overview on researches on underwater sensor networks: applications, current challenges and future trends," *Int. J. Electr. Comput. Eng.*, vol. 6, no. 3, Ju. 2016.

[3] A. Manigopal and R. Panneerselvam, "Underwater wireless sensor networks: a survey," *Int. J. Comput. Sci. Inf. Technol. Security*, vol. 2, iss. 6, 2012.

[4] Y. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, iss. 2, Feb. 2006.

[5] H. Choudhary, "Challenges of underwater wireless communications networks," [Online] Available: https://dspcommgen2.com/challenges-of-underwater-wireless-communications-networks/, Accessed on May 14, 2019.

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-853-2