Underwater Acoustic Communications Security
Project Proposal

Team 185

Advisor: Prof. Shengli Zhou
Alivia Grate (EE)
Brandon Gilbert (EE)
Kaitlyn King (EE)
Muhammad Samir (EE)
Introduction

Underwater Acoustic Networks (UANs) create numerous possibilities for communications below the surface of a body of water. However, because these networks operate in an open environment they are vulnerable to attack from various forms of interference and jamming. Malicious attempts to disrupt a communication channel will be the focus of this project. Using some prior research, Team 185 will attempt to identify the weaknesses in four different UAN systems with respect to their ability to receive a signal that is being jammed. Innovative ways to mitigate a jamming source will be designed once the major vulnerabilities are found and understood.

The initial requirements of this project are to identify the network vulnerabilities across underwater networks that use DSSS, FSK, S2C, and OFDM modulation. Frequency Shift Keying (FSK) is the oldest and best understood method, which has been secured to the degree that the military is confident using it. Direct Sequence Spread Spectrum (DSSS) is a very well developed technology but has security limitations and is not the most efficient with respect to bandwidth. Sweep Spread Carrier Technology (S2C) has promising security characteristics, that arise from the constant sweep of the signal. Lastly, Orthogonal Frequency Division Multiplexing (OFDM) offers very efficient use of bandwidth, and is currently used on most cell phone networks. These types of modulation need to be tested and fully understood before the group can proceed to improve each network’s defense measures.

The task of securing a UAN is a complicated problem due to several factors that are unique to underwater communication. Long propagation delays, narrow bandwidth, and multipath effects can degrade the performance of a UAN without the presence of a malicious attack. Additionally, security schemes cannot be directly applied from existing terrestrial networks to UANs. Modeling an aqueous environment accurately is also very difficult. This necessitates field testing in an environment that is at least similar to the intended deployment environment.

There are several specific types of electronic attacks that may be employed to disrupt one of these networks. Jamming attacks may be separated into three categories. A constant attack continuously injects noise or regular packets into a channel. A random attack, using either recorded signals or white noise, adjusts the gain of the jammer in a pseudo random fashion. Finally, a reactive attack only begins jamming when network activity is sensed. Moreover, we can classify jammers into two types that will use one of the above mentioned methods to disrupt a signal. A dummy attack jammer knows nothing about the network protocol being attacked and simply tries to corrupt packets using noise. The second type is known as a smart attack jammer. This type of jammer knows something, although not necessarily everything, about the network protocol being attacked. A smart attack jammer will pretend to be a legitimate node and attempt to control or corrupt packets. Once these vulnerabilities are understood based on collected data and research, the team will attempt to design a security system to mitigate as many types of attacks as possible while maintaining the performance of the network.
Underwater acoustic networks allow data to be transmitted wirelessly in underwater applications. A wireless network offers more possibilities for significant cost saving in comparison to more expensive underwater cabling. It also provides an option for extending the reach of an existing cabled network. Acoustic modems are available commercially from numerous companies (such as AquaSent, Evologics, Benthos, LinkQuest and more) that provide a variety of modems with different ratings. A simple underwater network is shown in figure (1) to demonstrate the communication phenomena underwater. As shown by figure (1), there is a transmitter and a receiver utilizing the same modulation scheme to communicate through acoustic waves. Modems consist of a transducer, an analog signal board, a digital signal processing board, and DC power supply (battery) all enclosed in waterproof housing. The transducer can transmit and receive signals, while the circuit boards are programmed to control the network channel and the battery is used to supply DC power. There is also a serial port on the modems that is used to interface with a computer (in this case).

UAN modems are used for many purposes by government agencies, research institutions and modern industries. Several extensive examples for the deployment of UANs include the
following: AUV/UUV tracking and communication, underwater construction, diver navigation and tracking, ocean monitoring (Sonar), research in marine biology, submarine communications, and lastly ROV (Remotely Operated underwater Vehicle) tracking and navigation.

These wireless networks are placed in open water and are vulnerable to external attacks. Research in securing underwater networks is an ongoing process which brings new ideas as the technology advances.

**Hardware**

As previously stated, four different types of modems are to be tested over the course of this project. The testing setup currently consists of three laptop computers (booted into Ubuntu or Windows), an external sampling card, a hydrophone, a signal jammer, and the modems to be tested. This is just an initial set up and is very likely to be changed for the inaudible modems, and more generally for all of the modems once we move the tests to the pool and later to the pond. The intended set up will include a network switch that will allow the test computer action to be synchronized via ad-hoc network. This will be changed to a wireless set up once it is working in a wired configuration. Additionally, a sampling card will be purchased or borrowed from the UWSN laboratory in order to record and analyze the inaudible signals produced by the Linkquest modems. The modems themselves are the most important part of the setup and are briefly described below.

The group is currently in possession of two AquaSeNT modems, which use orthogonal frequency division multiplexing (OFDM) modulation and operate in the audible frequency range of 14-20 kHz. These modems are an example of a parallel transmission system. Each sub carrier only occupies a small portion of total bandwidth. Furthermore, OFDM has the advantage of reducing frequency selective channel fading by employing frequency diversity.

There are currently two Teledyne Benthos ATM-885 modems available to the group in the lab. Additionally, the Benthos modems are being shared with a graduate group. This may make access and testing difficult at times. These modems are in the audible range as their low and middle frequency ranges are 9-14 kHz and 16-21 kHz respectively. They transmit data using Phase Shift Keying (PSK) at a max bit rate of 15,360 bits/sec. PSK is a modulation process that conveys data by changing the phase of a reference signal. Its benefits include having a high bandwidth efficiency. Although ATM-885 models can transmit using PSK, they only receive data using Multiple Frequency Shift Keying (MFSK). MFSK is a spread spectrum modulation process that transmits multiple tones simultaneously. This modulation only has a maximum bit rate of 2,400 bits/sec but it offers more reliability in a high multipath environment. ATM-885 modems are operable in depths up to 2,000 m.

The Evologics S2CR 18/34 underwater acoustic modem has been ordered for the second half of the project. Evologics is a German company that uses Sweep Spread Carrier (S2C) Technology to mimic the sound pattern of dolphins. This consists of spreading the signal over a wide range of frequencies which ultimately adapts the signal structure so that multipath components do not interfere with each other. This particular Evologics modem is a medium-range modem that operates in shallow waters up to 3500 meters, has a frequency band of 18 to 34 kHz and data transfer rates up to 13.9 kbits/second. This modem will be available to us for testing in the spring.

Linkquest UWM2000H is the fourth type of underwater acoustic modem that will be tested
for communication security weaknesses resulting in the modem’s vulnerability. There are two UWM2000H modems available for testing in the lab. These are medium range (1500 m.), low power modems that can be used up to 2000 meters deep under water. Moreover, they can also be used for long-range in shallow or very shallow environments with very harsh multipath conditions. Linkquest modems are implemented using Direct Sequence Spread Spectrum (DSSS), a modulation scheme in which the bandwidth is significantly larger than the information rate, and symbol sequence is combined with spreading sequence to get a baseband waveform. These modems are usually deployed for one or more of these reasons: antijamming, multiple access and bandwidth diversity. Our modem UWM200H operates in frequency range of 26 kHz - 45kHz (inaudible) and provides a data transfer rate of 300 to 1200 bits/second.

**figure (2)**

*Tank testing setup. This has been used as an initial starting point for modem testing, AquaSeNT (OFDM) are shown.*

Team 185, 5
Underwater Acoustic Communication Physical Layer Security

There are several challenges to UAN security at the physical layer. Among these are factors that are intrinsic to underwater communication. Long propagation delays in UANs are the result of the speed of a radio signal in air (roughly the speed of light) as compared to an acoustic signal in water. Additionally the propagation speed of a signal is dependant on whether or not the water is fresh. An acoustic signal in fresh water will travel at 1,497 m/s. However, in seawater the pressure, temperature, and salinity can increase or decrease the speed depending on each value. Generally, deeper in the ocean will be faster. Another challenge to UAN communication is the narrow bandwidth available for signals. The modems used on this project range from 12kHz to 45kHz, which is a small range by radio standards. The last UAN challenge is something called multipath effects. This happens as a result of signals reflecting off of the surface of the water as well as the bottom of the body of water. When multipath occurs, signals arrive at the receiving modem at slightly different times with the same message. This causes errors on the network. For this project only fresh water will be used, and other UAN challenges will be considered when necessary during the design of a security protocol. This project will also only focus on the physical layer and denial of service (DOS) type attacks.

There are essentially two types of attacks, a dummy (signal) jammer, and smart (Deceptive) attack, that affect the physical layer and are used in DOS. The dummy attack knows nothing about the protocols of the network and generates noise to corrupt packets. More simply this is broadcasting white noise and hoping the gain will be enough to stop signal on a network. The smart attack knows some information about the network protocols as this type of jammer will pretend to be a legitimate node. This can be realized by playing back recorded signals from the network being jammed. There are also three possible modes under which each of these attacks may occur. A constant attack will continually inject signals (noise or regular packets) into the communications channel. A random attack will alternate between attacking and sleeping in a pseudo-random fashion. This could also be achieved by changing the level of the jammers gain at random. Lastly, a reactive attack occurs by attempting to jam only after some network activity is sensed. This is considered to be more advanced. In order for these attacks to be effectively used or countered, the portion of signal most affected by an attempt jamm must be discovered and understood.

Effective jamming is really about disrupting the preamble in most cases. This was shown in previous studies conducted by Michael Zuba on some of these modems. He stated that the preamble is the most effective attacking point and also covered some more basic considerations for effective jamming. In order to jam effectively the following events should occur: First, detect the legitimate network signal. Next, start the jamming transmission, making the period of transmission long enough to destroy the message. And lastly, note or calculate the signal propagation time. However, depending on the type of jamming method and the level of jamming gain, the preamble may not be comprehensively true.

Initial Test Results

Team 185 has obtained initial test results using tank and air set ups for one type of modem.
thus far. Using the OFDM modems these results have shown that denial of service for an acoustic modem is very easy to accomplish. Air tests were conducted first as follows. Jamming signals were sent before the preamble, just after the preamble, towards the end of the signal and in the middle of the signal. These were all white noise signals. The last test conducted was to play back an erroneous message to attempt a jam. While sending the intended signal, message (a), between modems, message (b) which had been pre-recorded, was also sent to the receiving modem simultaneously. While the white noise jam was successful by increasing the gain regardless of the start time, the false message only jammed if the preamble of (b) interfered with the preamble of (a). The first three plots of figure (3) show a signal without any jamming, a signal with a noise jam at the end, and a signal with a jam at the beginning respectively. These were all created for data obtained during air testing.

![Air test results using AquaSeNT OFDM modem](image)

The next series of tests were conducted using the tank set up with the same modems. The results of the tests were very similar. However, the most noticeable difference was the team’s ability to control the gain of the jamming signal to nearly match the signal being sent by the modem. In contrast to the air tests, even with the gain of the jammer slightly less than that of the modem, the signals were still easily jammed by noise throughout the signal. Shown below by figure (4) are three frequency-time plots taken from data obtained during tank tests that show successful noise jams, and a successful signal jam. As with the air tests, spectrograms were also taken. However, as a result of the aqueous environment they are far more noisy and difficult to read.

![Tank Test Results using AquaSeNT OFDM modem](image)
Budget

Group 185’s total provided budget is $1000. So far, there have been only minor expenses, in the form of $20 worth of connectors from radio shack. An ethernet cable, a network switch, 12V batteries, a microphone, and all necessary software were provided by the School of Engineering with no cost to the group members. All modems, the jammers and the laptops have been provided by Professor Zhou and the Underwater Sensor Network (UWSN) Lab. There may be a potentially large expense in the form of recording equipment for inaudible signals for the Linkquest modems.

Timeline of Events