Short Paper: Launching Denial-of-Service Jamming Attacks in Underwater Sensor Networks

Michael Zuba, Zhijie Shi, Zheng Peng, and Jun-Hong Cui
Underwater Sensor Networks Lab, University of Connecticut,
115 North Eagleville Road, Storrs, CT 06269 USA
{michael.zuba, zhi, zhengpeng, jcui}@engr.uconn.edu

ABSTRACT
Recent surges in the development of Underwater Sensor Networks (UWSNs) have lead to a rapid acceptance of this technology in scientific, commercial, and military applications. However, there is limited work on secure communication mechanisms and techniques to protect these networks. Security mechanisms are widely studied in terrestrial networks and various defense mechanisms have been developed as safeguards. Due to the difference in communication mediums and physical environments, the existing solutions for terrestrial networks cannot be directly applied for UWSNs. In this paper, we study the effects of denial-of-service jamming attacks on UWSNs in real-world field tests. We develop our own jammer hardware and signals in order to analyze the characteristics of different jamming attack models on a network. Our tests are performed on existing commercial brand acoustic modems and an OFDM modem prototype. We show that UWSNs can be easily jammed using carefully timed attacks which are energy efficient.

Categories and Subject Descriptors
H.4 [Information Systems Applications]: Networks and Communication Theory; C.2 [Computer-Communication Networks]: Security and Protection; C.4 [Performance of Systems]: Performance Attributes

General Terms
Measurement, Design, Experimentation, Performance

1. INTRODUCTION
Terrestrial Wireless Sensor Networks (WSNs) and Underwater Sensor Networks (UWSNs) consist of spatially distributed sensors or devices that are capable of monitoring physical and environmental conditions such as humidity, temperature, and chemical/pollution contaminations. These sensors have changed the way humans live and are becoming more popular and feasible to integrate into our everyday lives. However, this surge of technology requires advanced security measures and techniques in order to provide defense against a malicious adversary wishing to tamper with these systems. A few adequate solutions for secure communication in WSNs have been introduced, ranging from complex cryptographic operations to trust based privacy schemes [1, 2]. However, communication interference, which is not addressable through conventional security mechanisms, can cause the network to be inoperable. Adversaries can observe communication between devices and exploit this knowledge of network transmissions to perform a type of denial-of-service (DoS) attack referred to as a jamming attack. Jamming attacks can simply ignore the network protocols being used and continually transmit on a wireless channel in the same frequency band to produce interference. Various solutions to jamming attacks in WSNs have been suggested from channel hopping to spatial retreat [3]. However, limited work has been done on studying the effects of jamming attacks on UWSNs.

UWSNs are uniquely characterized by their use of underwater acoustic channels since electromagnetic waves cannot propagate over long distances in the underwater environment [4]. However, underwater acoustic communication channels suffer from numerous inherent properties such as long propagation delays, narrow bandwidth and multipath effects. All of these factors create high error rates and affect the transport reliability [5]. Additionally, UWSNs suffer from rigid resource constraints, such as limited battery life and computational power. The dynamic nature of the aquatic environment also prevents any form of physical security or barrier and therefore limits the practicality of potential security mechanisms. These constraints indicate that UWSNs need custom security solutions as existing security solutions in WSNs cannot be directly applied because they do not take into consideration the above factors.

The underwater acoustic channel is an open environment which makes UWSNs more vulnerable to jamming attacks. In many cases, a receiver cannot tell the authorized signal from the jamming signal. Additionally, contrary to radio communications, there is no standard model for the acoustic communication channel underwater [6]. The channel conditions will be affected by various properties such as depth and temperature of the underwater environment. Therefore, it is required to study the feasibility of jamming attacks on UWSNs to understand the effects of the environment and how different jamming attacks affects the network.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 2011 ACM 978-1-4503-1151-9 ...$10.00.
A majority of the research on UWSNs is conducted through simulation and modeling. However, due to the inherent properties of the underwater acoustic communication channel, it is difficult to accurately model the network and characteristics of signals through simulations. Therefore, we focus on an experimental field test approach using AquaTUNE [7], our testbed system, and introduce various types of jamming attacks, as well as investigate their effects on UWSNs. With the creation of our own jammer, both hardware and signal, we perform real-world field tests to study the characteristics of each jamming attack, analyze how the jammer affects the performance of the network and evaluate how the network responds to such attacks. In our experiments, we perform two separate case studies using current commercial brand acoustic modems [8] and an OFDM modem prototype [9]. Finally, we analyze the transmission signal of both modems to determine when the jammer should attack to be most effective and energy efficient.

The rest of the paper is organized as follows. In Section 2 we provide related work. Section 3 introduces different jamming attack models. Section 4 discusses jamming signal characteristics, our jammer hardware and provides two case studies evaluating the effect of these attack models on a UWSN in real-world field tests. We also discuss the implications of our results. In Section 5 we provide our conclusions.

2. RELATED WORK

Limited work has been conducted on studying security mechanisms in UWSNs. We present a few related works below.

Kong et al. [10] explore the effects of wormhole attacks in underwater networks. A wormhole attack is where an adversary records a packet at one location in the network, tunnels it to another location, and replays the recorded packet. This attack can severely disrupt the network. The authors show that wormhole attacks of any length are low-cost, in terms of performing, and can disrupt communication in UWSNs that are longer or shorter than one-hop transmission ranges. Existing solutions for this attack in terrestrial networks are shown to be ineffective in preventing these attacks in UWSNs.

Wang et al. [11] propose a distributed approach to defend against wormhole attacks in UWSNs. The protocol, DisVoW, uses distances measured from the propagation delay of signals to construct a local network topology and visualizes distortions in edge lengths and angles. This protocol does not require any special hardware and simulations are used to evaluate its accuracy. DisVoW is a first step towards visualizing network topologies for wormhole defense.

Jamming attacks in WSNs have been extensively studied in terrestrial networks and still attract considerable attention for developing adequate solutions. We discuss a few related works below.

Xu et al. [12] proposes and evaluates four different jamming attack models that can be used to disrupt network performance. The authors evaluate the use of various network metrics, such as packet delivery ratio, packet send ratio, and signal strength, for detection of a jammer. It is observed that signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. The paper concludes that no single metric can be used to detect jamming attacks and that more enhanced detection protocols need to be developed.

Li et al. [13] studies the effect of a sophisticated jammer in a single-channel WSN. The jammer model used is where the jammer controls the probability of jamming and the transmission range in efforts to cause the maximum damage to a network. The jammer will also cease its attack once it has been detected by the network. This work introduces an understanding of the jamming problem by identifying tradeoffs and showing how manipulating different network and signal parameters affect the performance in jamming attack and detection methods.

It is clear by existing studies in WSNs that the jamming problem is deep and complex. Countermeasures involving various types of analysis and technologies have been introduced. However, to the best of the authors knowledge, there is no published work on studying the jamming problem in UWSNs.

3. JAMMING ATTACKS

Similar to terrestrial sensor networks, UWSNs are subject to jamming attacks when an adversary injects unwanted signals into the communication channels. These signals can occupy the communication channel such that legitimate communication cannot take place or corrupt the packets in transmission. In general, a jamming attack is an effective network disruption method because of the following three reasons:

- An attack can be performed by listening to the open communication medium and then broadcasting to the network;
- A well thought-out attack can drastically degrade the performance of a network while only incurring small costs to the attacker;
- In general, no special hardware is needed to launch a jamming attack.

3.1 Attack Models

Depending upon the signals being transmitted and how they are transmitted, a jammer can be categorized into two types: Dummy (Signal) Jammer and Smart (Deceptive) Jammer.

1) Dummy (Signal) Jammer: This type of jammer knows nothing about the underlying protocols of the network. It simply generates a signal that is garbled or noise to jam the communication channel and corrupt control/data packets. Since the acoustic communication channel is an open environment, a jammer can wreak havoc on the communication performance of a UWSN.

2) Smart (Deceptive) Jammer: This type of jammer knows some information about the network protocols being used and generally does not follow the underlying MAC protocol of the network. The jammer will use legitimate control/data packets instead of noise to create congestion or occupy the channel. This type of jammer will pretend to be a legitimate node in the network.
Taking after [12] both types of jammers can utilize the following attacks:

- **Constant Attack**: In this attack a jammer will continually inject radio signals (noise) or regular data packets into the communication channel to corrupt packets or congest the network;
- **Random Attack**: A jammer in this attack will alternate between sleeping and jamming the communication channel continually;
- **Reactive Attack**: This attack is considered more sophisticated. A jammer will remain idle when the communication channel is idle. When transmission activity is sensed the jammer will start transmitting to jam the network.

### 3.2 Network Metrics
In jamming attacks, a few network metrics have been identified as being potentially affected by the presence of a jammer [12]. Studying these metrics may give preliminary insights into the effect of a jamming attack. We introduce and define a few useful network metrics that will be studied in our analysis.

**Packet Delivery Ratio (PDR)** can be measured in multiple ways. It can be measured at the receiver node as the ratio of the number of packets that pass the cyclic redundancy check (CRC) check with respect to the number of packets received overall, at the sender as the ratio of acknowledgments received to those packets sent out by the sender or as the number of packets sent by the sender to the receiver over the number of packets the receiver actually received.

**Packet Send Ratio (PSR)** is measured as the ratio of packets that are sent out successfully by a source node compared to the number of packets that were intended to be sent out, as recognized by the medium access control (MAC) layer. Again, this metric will provide useful for analysis.

**Network Throughput (TP)** is directly related to PDR. It is the average rate of successful message delivery over the communication channel. Network throughput can also be measured as system throughput, which is the sum of data rates delivered to all nodes in the network.

### 4. EXPERIMENTAL STUDIES
In this section two case studies are presented on the effects of different jammers on a UWSN in real-world field tests. Additionally, we present a jamming scheme that limits energy consumption and transmission time to effectively jam the network by attacking the network at a certain time period.

#### 4.1 Jamming Commercial Brand Modems
We performed a preliminary study on the effects of various jamming attacks on our field testbed using Benthos ATM-885 commercial brand modems at a frequency band of 9-14 kHz [8]. The design of these commercial modems is based on multiple frequency-shift keying (MFSK).

In order to determine the most effective way to jam a UWSN using commercial modems, we tested numerous attack models. The type of jammer used was the dummy (signal) jammer and involved the use of four different attack models. These models are constant, random, reactive, and white noise jammers. The signal used for our jamming attacks in this experiment was a recorded version of a regular transmission from the commercial brand modems.

The hardware used to create our jammer consisted of an amplifier used to increase the signal power for proper underwater use that would match that of the acoustic modems being used, an ITC-1032 deep water omnidirectional transducer and a 12V battery to power the device. The amplifier allows for any input device to be used to generate a signal. The power consumption of our jamming equipment is 4 watts during idle state. At full transmission power, the jamming device has a power consumption of 4.476 watts.

We performed our experiments in Mansfield Hollow Lake, in Mansfield, Connecticut. In our experiments the network consisted of one sender and one receiver which are spaced 298.8 meters apart. The jammer was placed in four different positions: 400 meters, 298.8 meters, 167.3 meters, and 75 meters away from the receiver. BCMAC was the medium access control (MAC) protocol used in the network, with a sending rate of 0.04. The sending rate is based on a Poisson traffic generator that runs on the application layer. The traffic generator sends out data packets in such a way that the inter-departure time between two consecutive packets follows the Poisson distribution. Each jamming test was run for ten minutes with the power level of the nodes and jammer being set to 1 (an average transmit power of 2 watts), and the sender used packets with a length of 400 bytes. Tests were carried out for longer durations but we omit the results as there was no difference when increasing the length of the experiment.

<table>
<thead>
<tr>
<th>ATTACK</th>
<th>PDR (%)</th>
<th>PSR (%)</th>
<th>TP (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Operation</td>
<td>100</td>
<td>100</td>
<td>140.0660</td>
</tr>
<tr>
<td>Constant Jammer</td>
<td>0</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>Random Jammer</td>
<td>54</td>
<td>100</td>
<td>30.09</td>
</tr>
<tr>
<td>Reactive Jammer</td>
<td>0</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>White Noise</td>
<td>100</td>
<td>100</td>
<td>139.8205</td>
</tr>
</tbody>
</table>

Table 1: Network Performance

In our preliminary investigation we analyzed the variations of the network metrics in various network conditions. The results can be summarized in Table 1. The jammer was placed 298.8 meters away from the receiver for these tests. We measured the average PDR (in %), PSR (in %), and TP (in bits per second) in normal network conditions where no jammer is present and in network conditions where a jammer is present varying the attack model. In each test we allowed the first packet to get through to the receiver to ensure packets could be delivered. After the first packet was delivered the jamming attack was started.

We can observe a few interesting things from Table 1. First, we were not able to jam the network using an increased white noise level, no packets were lost. The network performed roughly the same as it would during normal operation. Sec-
Figure 1: Throughput of Jamming Attacks

ond, it is clear that constant and reactive attacks perform the best. However, the reactive attack model is much more energy efficient because it does not need to continually jam the network. We will further discuss these differences in Section 4.4. Third, while we could jam packets from being received at the receiver, we were unable to stop the network from actually transmitting packets. In Fig. 1 we plot the network throughput of each model from the entire first test, which are summarized in Table 1.

4.2 Efficient Jamming Scheme

We further studied the effects of jamming on UWSNs by investigating when an attack needed to be launched to effectively jam the network while minimizing energy consumption and the probability of detection. A diagram of the transmission signal being sent from the commercial modems can be seen in Fig. 2. The signal consists of two main parts. The first part is a preamble or header which lasts for roughly 1.5 seconds and sets up synchronization. The final part of the signal is where the actual data is sent out. The length of this transmission will vary based on the packet length size.

<table>
<thead>
<tr>
<th>TIME</th>
<th>0.5s</th>
<th>1s</th>
<th>1.5s</th>
<th>2s</th>
<th>3s</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAM</td>
<td>JAM</td>
<td>JAM</td>
<td>JAM</td>
<td>NO JAM</td>
<td>NO JAM</td>
</tr>
<tr>
<td>JAM</td>
<td>JAM</td>
<td>JAM</td>
<td>JAM</td>
<td>NO JAM</td>
<td>NO JAM</td>
</tr>
<tr>
<td>NO JAM</td>
<td>NO JAM</td>
<td>JAM</td>
<td>NO JAM</td>
<td>NO JAM</td>
<td>NO JAM</td>
</tr>
<tr>
<td>NO JAM</td>
<td>NO JAM</td>
<td>NO JAM</td>
<td>NO JAM</td>
<td>NO JAM</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Jammer Start Time vs. Distance from Receiver

Using the characteristics of this signal, we performed another set of experiments to determine the most effective time to attack the network. Our results can be summarized in Table 2. In this table we compare the starting time of the jamming attack versus the distance of the jammer from the receiver. The power levels were the same as the previous experiment discussed in Section 4.1. We observe that the most effective time to jam the network is during the preamble. Specifically, launching a jamming attack in the first second will ALWAYS jam the communication channel. During our experiments we tested a jamming signal consisting of 1 second of a recorded preamble and 1 second of our jamming signal from Section 4.1. Both were started at 0.5 seconds into the legitimate transmission signal. Each jamming signal was able to jam the network and prevent the receiver from obtaining any information from the sender.

Figure 2: General Signal Diagram

4.3 Jamming OFDM Modems

Multicarrier modulation in the form of orthogonal frequency division multiplexing (OFDM) has prevailed in recent broadband wireless systems over radio channels [14]. The success of OFDM in radio channels has motivated research in applying OFDM in underwater acoustic channels. Using a prototype version of an OFDM acoustic modem we conducted another set of experiments to analyze the effects of jamming attacks on these modems. The jammer type in these experiments was also a dummy (signal) jammer. The hardware used for the jammer in these experiments is an OFDM modem that is programmed to act as a jammer instead of a legitimate node. The jamming signal was a recorded sample of a preamble from the OFDM modem that lasts for 245 milliseconds.

In this experiment we had one sender and one receiver, which are placed 200 meters apart. The jammer was placed 200 meters away from the receiver. We use the same network parameters as mentioned in Section 4.1. We conducted similar experiments as in Section 4.2 to develop an efficient jamming scheme. A general signal diagram of the OFDM signal transmission can be seen in Fig. 3. The OFDM signal transmission consists of a detection preamble, a brief pause followed by a synchronization preamble and then transmission of the data in blocks. We introduced our jamming signal into the network during three different phases of the signal transmission. The first test was to transmit the jamming signal during the preamble of a legitimate transmission. The result of this experiment was that the jammer was successful as it caused a collision with the legitimate packet. The receiver did not receive any information and was unaware of the transmission. The second test was to transmit the jamming signal after the preamble during the legitimate transmission of the first data block. This caused the first data block to become corrupted and the receiver reported a decoding and CRC error. No data was able to be received. The final test was to transmit the jamming signal during the transmission of the second data block. This attack caused the same result as the previous attack. The receiver reported a decoding and CRC error and no data was able to be received.

Figure 3: Signal Diagram of OFDM Transmission
4.4 Discussions

Our experiments have shown that both the commercial brand modems and the OFDM modem prototype are vulnerable to malicious jamming attacks. However, it is important to note that reactive attacks could perform differently on the commercial brand modems depending on how long it takes an attacker to sense that the channel is being used. In our experiments, the attacker could sense the transmission almost immediately and was able to start transmitting its jamming attack without much delay. If an attacker takes longer to sense the channel transmissions then it is possible that the attacker will miss the opportunity to jam the channel.

\[ t_{\text{detect}} + t_{\text{start}} + t_{\text{jam}} \leq t_{\text{preamble}} \]  

(1)

It is also clear from our experiments that UWSNs can be jammed by overpowering the legitimate nodes with its own signal transmission. Essentially, a jammer could raise its power level to be greater than a legitimate node and this will often overwhelm the intended receiver causing it not to hear the legitimate transmission. However, this approach is not efficient in regards to energy conservation and detection constraints.

5. CONCLUSIONS

In this paper, we performed experimental real-world field tests to introduce and analyze various types of jamming attack models in UWSNs. The effectiveness of different jamming attack models were compared using network statistics. We created our own jamming attack signals and hardware to study the characteristics of each jamming attack and the performance of the network being attacked. Our tests were conducted on commercial brand modems and an OFDM modem prototype. Experimental results demonstrate that jamming attacks on UWSNs can easily be launched and drastically degrade the performance of the network. Our work provides the necessary initial stepping stone for studying the effectiveness of DoS jamming attacks in UWSNs which will allow researchers to use these new insights to develop adequate detection and mitigation schemes for these attacks.

6. REFERENCES