sensors

MDPI

Article

On Modeling Eavesdropping Attacks in Underwater Acoustic Sensor Networks †

Qiu Wang [1], Hong-Ning Dai [1,*], Xuran Li [1], Hao Wang [2] and Hong Xiao [3]

[1] Faculty of Information Technology, Macau University of Science and Technology, Macau; qiu_wang@foxmail.com (Q.W.); lxrget@163.com (X.L.)
[2] Big Data Lab, Faculty of Engineering and Natural Sciences, Norwegian University of Science & Technology in Aalesund, 6009 Aalesund, Norway; hawa@ntnu.no
[3] Faculty of Computer, Guangdong University of Technology, Guangzhou 510006, China; wh_red@gdut.edu.cn
* Correspondence: hndai@ieee.org; Tel.: +853-8897-2154
† This paper is an extended version of our paper published in Wang, Q.; Dai, H.N.; Li, X.; Wang, H. Eavesdropping attacks in underwater acoustic networks. In Proceedings of the 10th International Conference on Information, Communications and Signal Processing (ICICS), Singapore, 2–4 December 2015.

Academic Editor: Rongxing Lu
Received: 17 March 2016; Accepted: 11 May 2016; Published: 18 May 2016

Abstract: The security and privacy of underwater acoustic sensor networks has received extensive attention recently due to the proliferation of underwater activities. This paper proposes an analytical model to investigate the eavesdropping attacks in underwater acoustic sensor networks. Our analytical framework considers the impacts of various underwater acoustic channel conditions (such as the acoustic signal frequency, spreading factor and wind speed) and different hydrophones (isotropic hydrophones and array hydrophones) in terms of network nodes and eavesdroppers. We also conduct extensive simulations to evaluate the effectiveness and the accuracy of our proposed model. Empirical results show that our proposed model is quite accurate. In addition, our results also imply that the eavesdropping probability heavily depends on both the underwater acoustic channel conditions and the features of hydrophones.

Keywords: security; eavesdropping; underwater acoustic sensor networks; isotropic hydrophones; array hydrophones

1. Introduction

With the proliferation of various underwater applications such as underwater environment monitoring, offshore structural health monitoring and target tracking, underwater acoustic sensor networks (UASNs) have received much attention. Due to the high attenuation of electromagnetic waves in underwater environments, acoustic communications are typically used in underwater sensor networks. Recently, security has become one of the important concerns in UASNs [1]. We summarize related works on security of UASNs as follows.

1.1. Related Works

There are a number of studies on UASNs. In particular, a review of the early history of the acoustic underwater communication was presented in [2]. Research advances and challenges in underwater sensor networks with acoustic communications were summarized in [3]. Generally, the studies on UASNs can be mainly divided into three categories. The first category focused on analyzing the performance of UASNs [4–7]; the second category focused on improving the network performance in Medium Access Control (MAC) layer [8–10]; the third category focused on designing routing

schemes [11–13]. Underwater cognitive acoustic networks were proposed in [14] to improve the spectrum reuse of acoustic communications. However, there are few studies investigating the network security of UASNs. In particular, a novel secure scheme was proposed to secure the underwater acoustic sensor networks in [15]. The wormhole attack was investigated in [16]. One of vulnerabilities of UASNs was found in [17] that UASNs are suffering from denial-of-service jamming attacks.

On the other hand, as one of the typical security threats in *terrestrial* wireless sensor networks, eavesdropping attacks have received extensive attention recently. It is difficult to detect the eavesdroppers since they just passively wiretap the transmissions without disclosing their existence. Many malicious attacks often follow the eavesdropping activities [18]. Encryption is one of the most commonly used techniques to protect the confidential communications in cellular networks (e.g., Cellular Message Encryption Algorithm [19]), wireless local area networks (e.g., WEP [20], WPA and WPA2 [21]) and wireless personal area networks (WPAN) [22]. However, encryption algorithms may not be feasible to wireless sensor networks since sensor nodes have the energy constraints and computational constraints [23].

In addition to message encryption, there are a number of anti-eavesdropping countermeasures [24–32]. In particular, it is shown [24] that to adjust transmitting power can reduce the eavesdropping risk. Besides, [26–29] found that using directional antennas in wireless sensor networks can enhance the security. Moreover, to deliberately send spurious messages or (dummy data) [25] can also effectively reduce the eavesdropping success rate. Other anti-eavesdropping schemes include the use of defensive jammers [31,32] to protect the normal transmissions.

It is necessary to investigate the eavesdropping behaviors conducted by eavesdroppers since we can offer better protection on the confidential communications if we have a better knowledge on the eavesdroppers [33,34]. For example, we only need to encrypt the communications in the area or the direction that is vulnerable to eavesdropping attacks so that the security cost can be significantly saved.

However, to the best of our knowledge, there is no study on investigating the eavesdropping attacks in UASNs. The previous analytical models on investigating the eavesdropping activities in terrestrial wireless sensor networks [30,35] can not be used to UASNs due to the different features of acoustic signals in underwater environments. For example, the path loss effect of an underwater acoustic channel depends on both the distance and the signal frequency. However, the terrestrial radio channel is independent of the radio signal frequency. Therefore, this is the goal of this paper to establish a novel analytical model and to investigate the eavesdropping activities in UASNs.

1.2. Major Contributions

Generally, in conventional UASNs, each node is equipped with an *isotropic hydrophone*, which collects acoustic signals in all directions. We call such underwater acoustic sensor networks with isotropic hydrophones as *IUSNs*. Compared with an isotropic hydrophone, an *array hydrophone* can collect acoustic signals on desired direction. In other undesired directions, there are no signal or weakened signal. Thus, using array hydrophones in UASNs can potentially reduce the interference and consequently improve the network performance. For example, it is shown in [36] that using array hydrophones in UASNs can significantly improve the network throughput. We call such underwater acoustic sensor networks with array hydrophones *AUSNs*. In this paper, we investigate the eavesdropping activities in both IUSNs and AUSNs. We also consider two cases in which an eavesdropper is equipped with an isotropic hydrophone and an array hydrophone, respectively. We name an eavesdropper with an isotropic hydrophone as an isotropic eavesdropper and name an eavesdropper with an array hydrophone as an array eavesdropper.

Our major research contributions in this paper can be summarized as follows.

- We formally propose an analytical model to investigate the probability of eavesdropping attacks in both IUSNs and AUSNs with consideration of underwater acoustic channel conditions, including signal attenuation and ambient noise. In particular, we establish the relationship between the *eavesdropping success condition* and the underwater acoustic signal channel. We further derive the eavesdropping probability with consideration both isotropic eavesdropper and array eavesdropper, respectively.
- We conduct extensive simulations to validate the effectiveness and the accuracy of our proposed model. The simulation results match the analytical results, indicating that our proposed model is accurate.
- We compare the eavesdropping probability of IUSNs and AUSNs. In particular, we find that the eavesdropping probability of AUSNs is lower than that of IUSNs, implying that using array hydrophones in UASNs can reduce the eavesdropping probability. We also find that an array eavesdropper has a higher eavesdropping probability than an isotropic eavesdropper in both IUSNs and AUSNs.
- We find that the eavesdropping probability heavily depends on the acoustic signal frequency, spreading factor, wind speed and the node density. Our results pave the way for designing a better protection mechanism in UASNs.

The rest of this paper is organized as follows. Section 2 first presents the channel model in underwater acoustic communications. We then introduce the transducer used in this paper in Section 3. We next analyze the eavesdropping attacks in UASNs in Section 4. Section 5 gives the empirical results with comparison of IUSNs and AUSNs considering two kinds of eavesdroppers. Finally, we conclude the paper in Section 6.

2. Underwater Acoustic Channel Model

In this section, we first instroduce the attenuation of underwater acoustic signal in Section 2.1, and then present the impacts of the ambient noise in Section 2.2.

2.1. Attenuation

The attenuation in underwater acoustic communications is characterized by a path loss that depends not only on the distance between the transmitter and the receiver, but also on the signal frequency. In particular, the path loss or the attenuation that occurs in an underwater acoustic channel over a distance d for a signal of frequency f is given by [37]:

$$A(d,f) = d^k \alpha(f)^d \tag{1}$$

where k is the spreading factor (ranging from 1 to 2) and $\alpha(f)$ is the absorption coefficient of signal frequency f. Note that the different values of k describe the different scenarios of geometry of propagation: $k = 1$ for cylindrical spreading; $k = 2$ for spherical spreading.

Usually, Equation (1) can be expressed in dB as follows:

$$10\log A(d,f) = k \times 10\log d + d \times 10\log \alpha(f) \tag{2}$$

Generally, if the frequency f is above a few hundred Hz, the absorption coefficient $10\log\alpha(f)$ in dB/km for f in kHz can be expressed as follows:

$$\begin{aligned} 10\log\alpha(f) = 0.11 \times \frac{f^2}{1+f^2} + 44 \times \frac{f^2}{4100+f^2} \\ +2.75 \times 10^{-4} f^2 + 0.003 \end{aligned} \tag{3}$$

For the lower frequency f, we have the absorption coefficient $10\log\alpha(f)$ as follows [38]:

$$10\log\alpha(f) = 0.002 + 0.11 \times \frac{f^2}{1+f^2} + 0.011f^2 \tag{4}$$

2.2. Ambient Noise

The ambient noise in underwater acoustic channel is more complicated than that in terrestrial wireless channel. We usually model the ambient noise by four kinds of sources: turbulence, shipping activities, waves, and thermal noise. Specifically, the noise caused by shipping activities can be modeled by shipping activity factor s, whose value ranges from 0 to 1 representing the intensity of shipping activities (0 representing low and 1 representing high). The noise of waves, aroused by wind, can be described by wind speed w (m/s). In UASNs, the ambient noise depends on signal frequency f and the formula between power spectral density of the four noise sources and frequency in kHz in dB re μ Pa per Hz are given by [38].

$$\begin{aligned} 10\log N_t(f) &= 17 - 30\log(f) \\ 10\log N_s(f) &= 40 + 20(s-0.5) + 26\log(f) - 60\log(f+0.03) \\ 10\log N_w(f) &= 50 + 7.5w^{1/2} + 20\log(f) - 40\log(f+0.4) \\ 10\log N_{th}(f) &= -15 + 20\log(f) \end{aligned} \tag{5}$$

where $N_t(f)$, $N_s(f)$, $N_w(f)$ and $N_{th}(f)$ denote the noise sources caused by turbulence, shipping activity, wind and thermal, respectively.

Then, the total noise in dB is as follows:

$$10\log N(f) = 10\log(N_t(f) + N_s(f) + N_w(f) + N_{th}(f)) \tag{6}$$

Figure 1 shows the power spectral density of the ambient noise $N(f)$(dB) in various values of shipping activity s and wind speed w. It can be seen from Figure 1 that shipping activity factor s mainly affects the noise when $0.001 < f < 1$ kHz, while wind speed w mainly affects the noise when $f > 1$ kHz, which is the frequency band usually used in underwater communications. Therefore, we will consider the impacts of wind speed w on the eavesdropping activities in this paper.

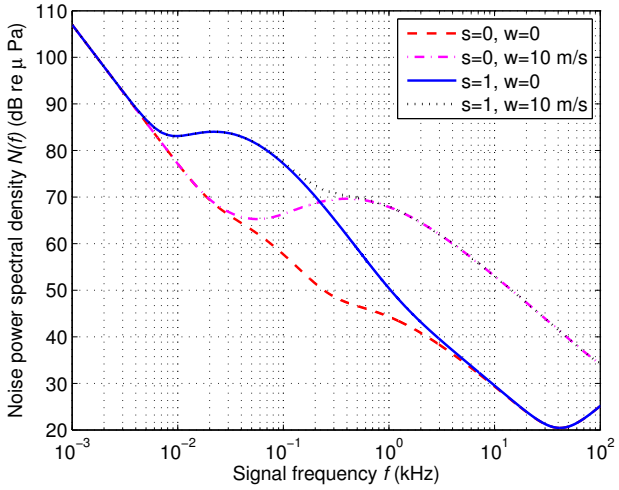

Figure 1. Power spectral density of the ambient noise $N(f)$ (dB re μ Pa).

3. Transducers

In UASNs, transducers are not only used to implement the conversion of acoustic energy into electrical energy or vice versa, but also used to transmit/receive acoustic signals. Transducers used as receivers are called hydrophones, and those used for transmitting are called transmitters or projectors [39]. In this paper, we focus on hydrophones. Conventional UASNs are commonly equipped with a single isotropic hydrophone which collects acoustic signals uniformly in all directional. Different from a single isotropic hydrophone, modern transducers are comprised of an array of hydrophones which receive signals more effectively in some directions (*i.e.*, improving signal noise ratio in some directions). Moreover, with the evolution of VLSI, modern hydrophones are able to form beams in desired directions. Thus, this section will introduce these two types of hydrophones.

An isotropic hydrophone collects acoustic signal uniformly in all directions. In particular, Figure 2 shows the beam pattern of an isotropic hydrophone.

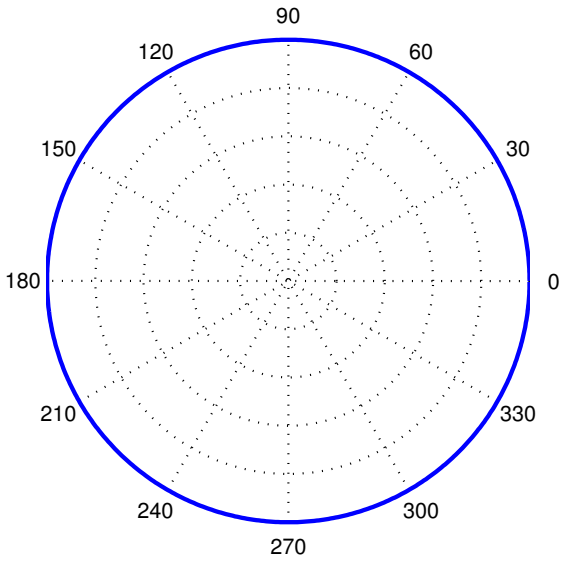

Figure 2. The beam pattern of an isotropic hydrophone.

An array hydrophone consists of an array of isotropic hydrophones. To model the characteristics of an array hydrophone, we introduce *Array Gain*, which is the improved gain on signal-to-noise ratio (SNR) compared with an isotropic hydrophone. The array gain can be expressed as follows [39]:

$$AG = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} a_i a_j \beta_s^{ij}}{\sum_{i=1}^{M}\sum_{j=1}^{M} a_i a_j \beta_n^{ij}} \tag{7}$$

where M is the number of isotropic hydrophone elements of an array hydrophone, a_i and a_j are the amplitude shading coefficients of the i-th hydrophone element and the j-th hydrophone element, respectively. If array hydrophones are unshaded, $a_i = a_j = 1$. β_s^{ij} is the correlation of the received signals between the i-th hydrophone element and the j-th hydrophone element and β_n^{ij} is the correlation of the noise between the i-th hydrophone element and the j-th hydrophone element.

One of most commonly used array hydrophones is an unshaded uniform linear array transducer, which consists of M isotropic hydrophones evenly spaced in a line, as shown in Figure 3. In this structure, l is the distance between two neighboring elements, and λ is the wavelength of acoustic

wave radiated from signal source (denoted by the blue star in Figure 3). In underwater communication, a signal wave is usually considered as a plane wave, meaning that signals can be received by each hydrophone element in the same direction θ. Although plane waves cannot be generated in practice, both spherical and cylindrical waves approximate plane waves when they are sufficiently far from signal source [39]. Therefore, we consider acoustic signal as a plane wave in this paper.

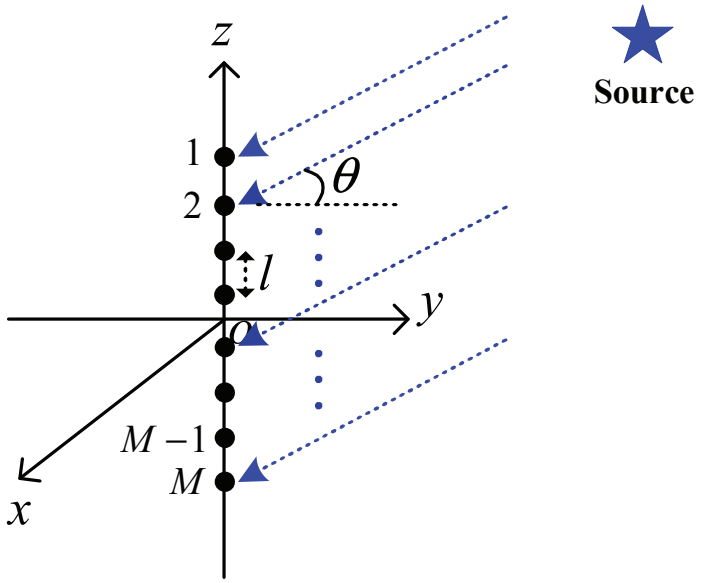

Figure 3. A line array hydrophone with M isotropic hydrophone elements.

Given this unshaded uniform linear array hydrophone, β_s^{ij} is described as follows:

$$\beta_s^{ij} = \cos(\frac{2\pi}{\lambda} |i-j| \, l \sin\theta) \tag{8}$$

where $|\cdot|$ denotes the absolute value.

In this paper, we consider that the array hydrophone uses a location identification scheme to acquire the direction of signal source and then adjust their angles to transmitters. Thus, we have $\theta = 0$. Then we apply this value in Equation (8) and obtain the correlations of received signal $\beta_s^{ij} = 1$.

In general, we consider omni-directional noise, meaning that noise surround each hydrophone with constant power in all directions. Then, the correlations of received noise β_n^{ij} is expressed by

$$\beta_n^{ij} = \begin{cases} 1 & i = j \\ \frac{\sin(\frac{2\pi}{\lambda}|i-j|l)}{\frac{2\pi}{\lambda}|i-j|l} & i \neq j \end{cases} \tag{9}$$

A common choice of the distance between the two neighboring isotropic hydrophone elements is $l = \frac{\lambda}{2}$. Applying the value in Equations (8) and (9) and combining with Equation (7), we then get $AG = M$. This means that an unshaded uniform linear array hydrophone can improve M times of signal-to-noise ratio compared to a single isotropic hydrophone, which is an important factor used in our analysis. The beam pattern of an unshaded uniform linear array hydrophone with 10 elements is shown in Figure 4.

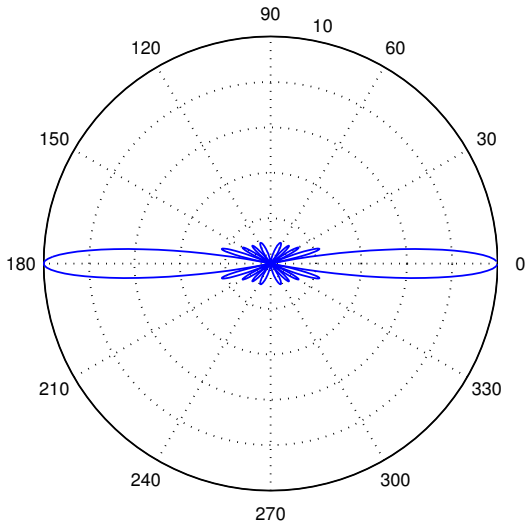

Figure 4. The beam pattern of an unshaded uniform liner array hydrophone with 10 isotropic hydrophone elements.

4. Analysis of Eavesdropping Attacks in UASNs

In our eavesdropping model, we consider two scenarios of UASNs according to the two different types of hydrophones: Scenario (i), in which every node is equipped with a single isotropic hydrophone; Scenario (ii), in which every node is equipped with an unshaded uniform linear array hydrophone. Scenario (i) and Scenario (ii) correspond to IUSNs and AUSNs, respectively. In addition, we consider that all the nodes are randomly distributed in a 2-D plane according to a homogeneous Poisson point process with density ρ in both IUSNs and AUSNs. Then, we consider two types of eavesdroppers: isotropic eavesdroppers and array eavesdroppers in both IUSNs and AUSNs. Recall that an isotropic eavesdropper is equipped with a single isotropic hydrophone and an array eavesdropper is equipped with an unshaded uniform linear array hydrophone. Thus, we investigate the impacts of different eavesdroppers on the eavesdropping probability of IUSNs and AUSNs, respectively.

Before we analyze eavesdropping activities, we have to analyze link criteria in both IUSNs and AUSNs in Section 4.1 and then derive eavesdropping success condition in Section 4.2. We next derive the eavesdropping probability in Section 4.3.

4.1. Link Criteria

We first define the link condition in UASNs. We denote the transmission power by P_t. The signal-to-noise ratio at receiver denoted by SNR can be calculated according to the aforementioned underwater acoustic channel model in Section 2 as follows:

$$SNR = AG\frac{P_t}{\int\limits_B A(d,f)df \int\limits_B N(f)df} \tag{10}$$

where B is the bandwidth used in acoustic communications. In order to investigate the relationship between frequency f and SNR better, we normalize the bandwidth. Then the Equation (10) can be simplify to

$$SNR = AG\frac{P_t}{A(d,f)N(f)} \tag{11}$$

Equation (11) is a general equation in both IUSNs and AUSNs. But note that in IUSNs, $AG = 1$, while in AUSNs, $AG = M$. Equation (11) can be expressed in terms of dB by SNR_{dB} as

$$SNR_{dB} = 10\log AG + 10\log P_t - 10\log A(d,f) - 10\log N(f) \tag{12}$$

Generally, a link can be successfully established if and only if

$$SNR_{dB} \geq \Delta_0(dB) \tag{13}$$

where Δ_0 is the minimum signal-to-noise ratio at receiver. In particular, we let the signal-to-noise ratio equal to Δ_0, and then have the minimum transmission power P_t in dB

$$10\log P_t = \Delta_0 + 10\log A(d,f) + 10\log N(f) - 10\log AG \tag{14}$$

We denote the minimum transmission power in IUSNs by P_t^i and that in AUSNs by P_t^a. Then, we can express the relationship between P_t^i and P_t^a from Equation (14) with different value of AG as

$$10\log P_t^a = 10\log P_t^i - 10\log M \tag{15}$$

In this paper, we assume that both AUSNs and IUSNs apply power control scheme to save power. In other words, the nodes in AUSNs and IUSNs use the minimum transmission power P_t^i and P_t^a, respectively. We can see from Equation (15) that the transmitters in AUSNs can use less transmission power to establish link under the same network topology and environment conditions compared with the transmitters in IUSNs.

4.2. Eavesdropping Success Condition

We now define the eavesdropping success condition that determines whether an eavesdropper can successfully wiretap the communication between a transmitter and a receiver. It is obvious that the eavesdropper can tap information implying that the eavesdropper can establish a link with a node. Thus, the eavesdropper can successfully tap information if and only if it fulfill Equation (13). Combining Equations (2), (12) and (13), we can have

$$k \times 10\log d + d \times 10\log \alpha(f) + 10\log N(f) - 10\log AG \leq 10\log P_t - \Delta_0 \tag{16}$$

where $AG = 1$ when networks with an isotropic eavesdropper and $AG = M$ when networks with an array eavesdropper. We observe that left-hand-side (LHS) of Equation (16) is an increasing function of the distance d. If we let LHS of Equation (16) be equal to right-hand-side (RHS), we then can obtain the *maximum eavesdropping distance* $d_{\max}$, within which an eavesdropper can wiretap a transmission successfully.

Generally, it is *non-trivial* to obtain the exact expression of $d_{\max}$ since Equation (16) is a transcendental function of d. However, we observe from Equation (16) that it is not difficult to obtain the numerical results of $d_{\max}$ when the frequency f, environment parameters (spreading factor k, and wind speed w) and the transmission power P_t are given.

Thus, we calculate $d_{\max}$ with different frequency f, k and w with the threshold of signal-to-noise $\Delta_0 = 20$ dB [38] and $P_t = 100$ dB considering an isotropic eavesdropper and an array eavesdropper ($M = 10$), respectively. The numerical results are presented in Figure 5. Specifically, we can see from Figure 5 that an isotropic eavesdropper (red dash lines) have higher $d_{\max}$ than an array eavesdropper (blue solid lines). Besides, $d_{\max}$ varies with different signal frequency f when environment parameters (spreading factor k, and wind speed w) are fixed. Furthermore, as shown in Figure 5, when the spreading factor k is fixed, increasing wind speed w leads to decreasing $d_{\max}$. This is the result of the higher noise when wind speed w is higher. It can also be seen from Figure 5 that with the fixed wind

speed w, $d_{\max}$ decreases with the increased spreading factor k. The reason is that increasing spreading factor k leads to higher absorption of the acoustic signal.

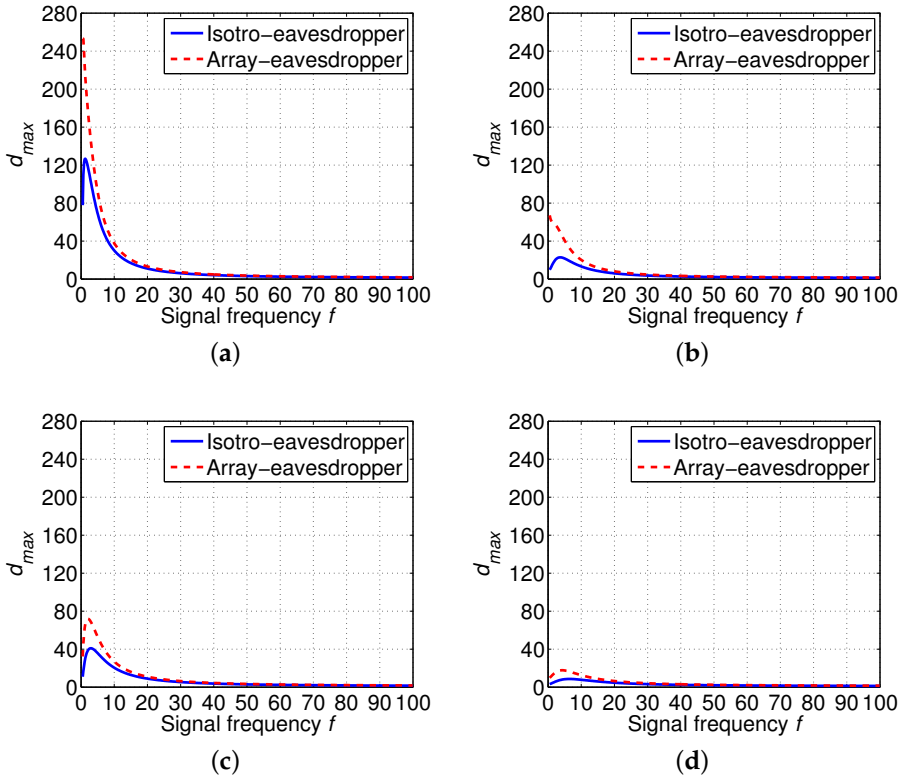

Figure 5. Maximum eavesdropping distance $d_{\max}$ (km) according to different signal frequency f (kHz) based on different spreading factor k and wind speed w when $P_t = 100\,\text{dB}$, $\Delta_0 = 20\,\text{dB}$. (**a**) $k = 1$, $w = 0\,\text{m/s}$; (**b**) $k = 1$, $w = 10\,\text{m/s}$; (**c**) $k = 2$, $w = 0\,\text{m/s}$; (**d**) $k = 2$, $w = 10\,\text{m/s}$.

4.3. Eavesdropping Probability

We model the successful chance of eavesdropping attacks by the *eavesdropping probability*, denoted by $P(E)$. To derive $P(E)$, we need to calculate the probability of no node being eavesdropped first. We then consider an *effective eavesdropping area* D, which is the expected value of the critical region where the communication can be wiretapped by eavesdroppers only when a node falls in this region. Since the eavesdropper is equipped with a single isotropic hydrophone, it wiretaps acoustic signals uniformly in all directions, as shown in Figure 6. In particular, we have

$$D = \pi d_{\max}^2 \tag{17}$$

where the value of $d_{\max}$ can be calculated by Equation (16).

We next denote the number of nodes in the eavesdropping area by a random variable Y. Since nodes are randomly distributed in a 2-D area according to a homogeneous Poisson point process, we then have the probability of no node falling in the eavesdropping area, which is given by

$$P(Y = 0) = e^{-\rho D} \tag{18}$$

Substituting D in Equation (18) by RHS of Equation (17), we finally obtain the *eavesdropping probability* $P(E)$ by the following equation:

$$P(E) = 1 - P(Y = 0) = 1 - e^{-\rho\pi(d_{\max})^2} \tag{19}$$

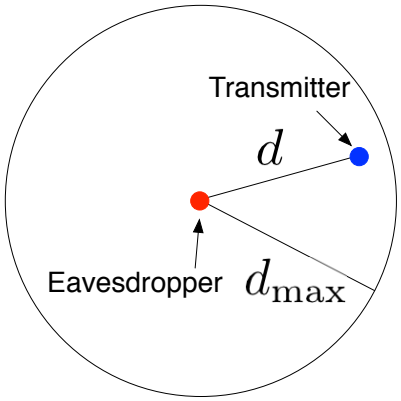

Figure 6. Eavesdropping region is a circle with radius $d_{\max}$.

From the aforementioned analysis, the higher spreading factor k and the higher wind speed w, the shorter the maximum eavesdropping distance $d_{\max}$ is. Therefore, we can see from Equation (19) that with the fixed node density ρ, the higher spreading factor k and the higher wind speed w, the lower probability of eavesdropping attacks $P(E)$ is. Our empirical results will further confirm this observation.

5. Empirical Results

In this section, we conduct extensive simulations to evaluate the accuracy and the effectiveness of our proposed analytical model. As indicated in the previous work [40], the border effect often affects the accuracy of the simulation results. In this paper, we consider a simplified approach to eliminate the border effect. Specifically, we place the eavesdropper at the center of simulation area, which is large enough so that the border effect can be ignored.

The statistical eavesdropping probability denoted by $P_s(E)$ is calculate by the following equation

$$P_s(E) = \frac{\text{No. of topologies that have been eavesdropped}}{\text{No. of topologies}} \tag{20}$$

The physical meaning of Equation (20) is the percentage of the number of topologies being eavesdropped to the total number of topologies. As shown in the previous work [40], when the total number of topologies $\to \infty$, we can accurately approximate the theoretical result. In practice, we generate $10,000$ random topologies for each run of simulations in this paper (to balance the accuracy against the computational complexity).

Then, we conduct extensive simulations by dividing them into two groups according to impacts of different eavesdropper: isotropic eavesdropper and array eavesdropper ($M = 10$). In each group, we investigate the eavesdropping probability in IUSNs and AUSNs, respectively. Note that we assume both IUSNs and AUSNs have the same network topologies and environment conditions with a fixed threshold of signal-to-noise threshold $\Delta_0 = 20\,\text{dB}$.

5.1. Eavesdropping Probability with an Isotropic Eavesdropper

We first conduct the first group of simulations with consideration of an isotropic eavesdropper in IUSNs and AUSNs, respectively.

5.1.1. Eavesdropping Probability in IUSNs

Figure 7 shows the simulation results of eavesdropping probability in IUSNs with an isotropic eavesdropper. We assign the acoustic signal frequency f with 10 kHz, 30 kHz and 90 kHz under

different values of spreading k and wind speed w and we fix the reference transmission power $P_t^i = 100\,\text{dB}$. In particular, the analytical results are shown as curves and the simulation results are shown as markers. We can see from Figure 7 that there is an excellent agreement of the simulation results with the analytical results. This indicates that our proposed analytical model is accurate. Besides, as shown in each curve of Figure 7, the eavesdropping probability increases with the node density ρ. This phenomenon can be explained by Equation (19), *i.e.*, the more nodes, the higher the chance of being eavesdropped.

Furthermore, we compare the results with different values of frequency $f = 10\,\text{kHz}$, $f = 30\,\text{kHz}$ and $f = 90\,\text{kHz}$, denoted by the blue, red and black curves, respectively. More specifically, we find that the eavesdropping probability decreases with the increased values of frequency f. This is because the acoustic signal attenuation goes much faster with the increased signal frequency in underwater environment when f is high (*i.e.*, $f > 8\,\text{kHz}$). Moreover, Figure 7 also shows that the eavesdropping probability decreases when wind speed w increases or spreading factor k increases. This trend confirms our aforementioned observation in Section 4.

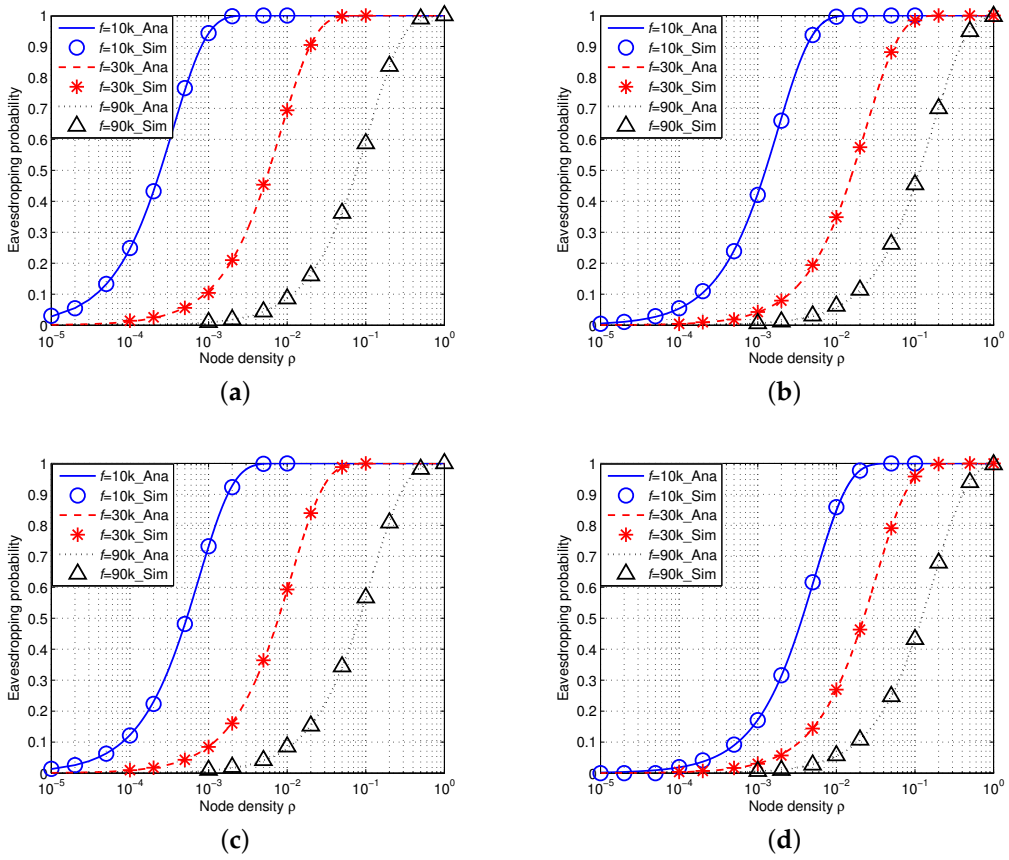

Figure 7. Eavesdropping probability in IUSNs with an *isotropic* eavesdropper versus node density ρ ($/\text{km}^2$) when $f = 10$ kHz, $f = 30$ kHz and $f = 90$ kHz under different spreading factor k and wind speed w. (**a**) $k = 1, w = 0\,\text{m/s}$; (**b**) $k = 1, w = 10\,\text{m/s}$; (**c**) $k = 2, w = 0\,\text{m/s}$; (**d**) $k = 2, w = 10\,\text{m/s}$.

5.1.2. Eavesdropping Probability in AUSNs

We then conduct simulations on the eavesdropping probability in AUSNs with an array eavesdropper ($M = 10$). Figure 8 shows the results. Note that the transmission power in AUSNs can be calculated by Equation (15) and the reference transmission power is $P_t^i = 100\,\text{dB}$. Similarly, we can also draw a conclusion that our analytical framework can accurately model the eavesdropping

probability in AUSNs as the simulation results match the analytical results. Besides, we can see that the eavesdropping probability increases with the increased node density ρ and decreases with the increased signal frequency f, and eavesdropping probability decreases when wind speed w or spreading factor k increases. Moreover, if we compare the eavesdropping probability in IUSNs with that in AUSNs together (by aligning Figures 7 and 8 together), we can find AUSNs have the lower values in terms of eavesdropping probability than IUSNs, implying that the nodes have less chance of being eavesdropped upon in AUSNs than that in IUSNs.

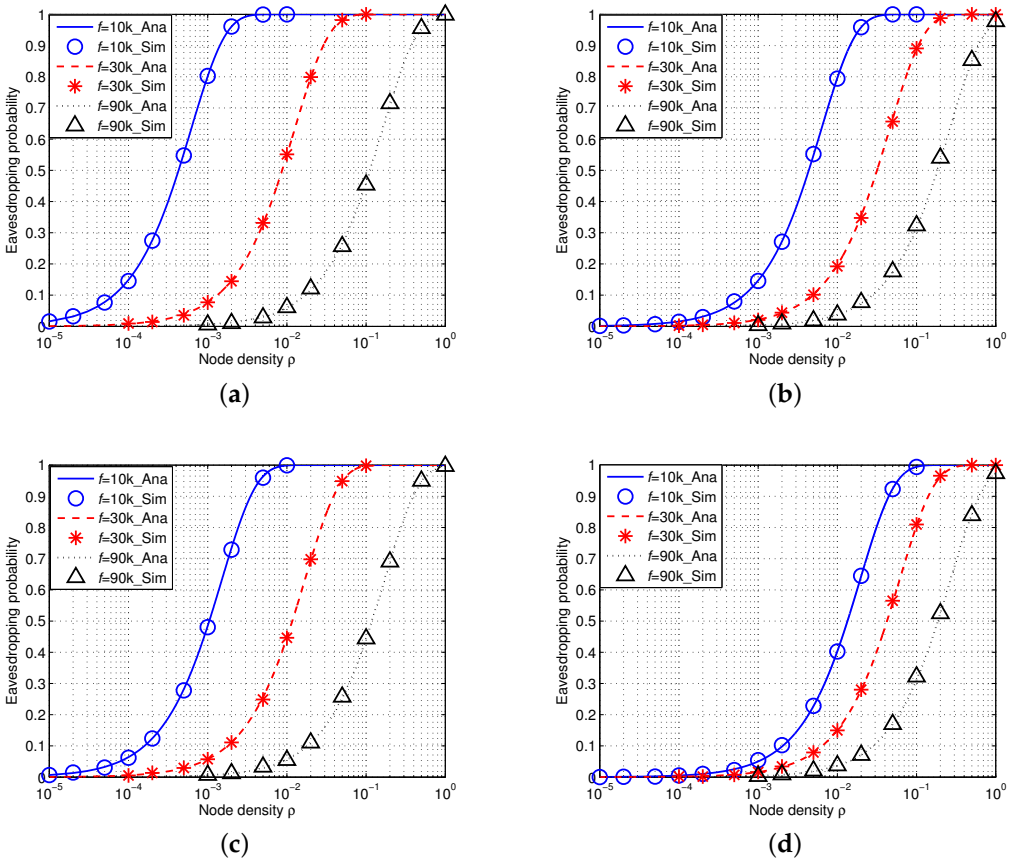

Figure 8. Eavesdropping probability in AUSNs with an *isotropic* eavesdropper versus node density ρ (/km^2) when $f = 10$ kHz, $f = 30$ kHz and $f = 90$ kHz under different spreading factor k and wind speed w. (**a**) $k = 1$, $w = 0$ m/s; (**b**) $k = 1$, $w = 10$ m/s; (**c**) $k = 2$, $w = 0$ m/s; (**d**) $k = 2$, $w = 10$ m/s.

5.2. Eavesdropping Probability with an Array Eavesdropper

We then conduct another group of simulations with consideration of an array eavesdropper in IUSNs and AUSNs, respectively.

5.2.1. Eavesdropping Probability in IUSNs

Figure 9 shows the simulation results of eavesdropping probability in IUSNs with an array eavesdropper. There is an excellent agreement of the simulation results with the analytical results, further confirming the accuracy of our model. Similarly, as shown in Figure 9, the eavesdropping probability increases with the node density ρ and decreases with the increased values of frequency f. Figure 9 also shows that the eavesdropping probability decreases when wind speed w increases or spreading factor k increases.

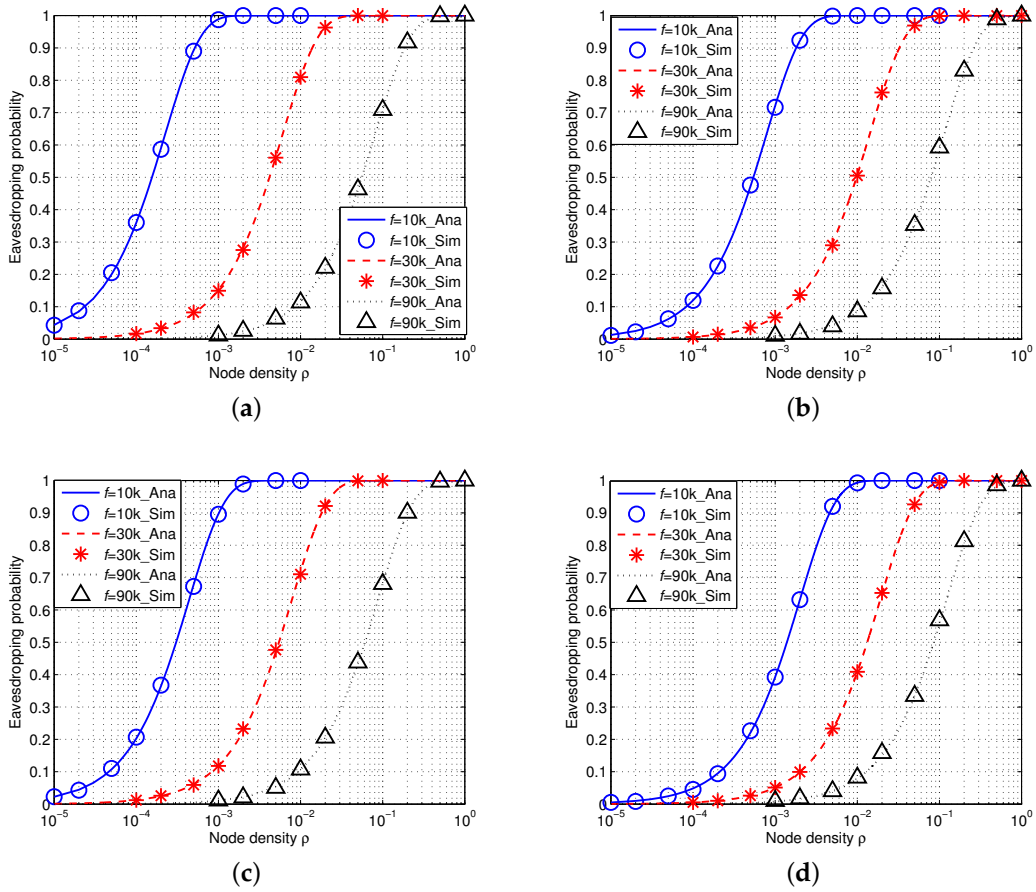

Figure 9. Eavesdropping probability in IUSNs with an *array* eavesdropper versus node density ρ ($/\text{km}^2$) when $f = 10$ kHz, $f = 30$ kHz and $f = 90$ kHz under different spreading factor k and wind speed w. (**a**) $k = 1$, $w = 0\,\text{m/s}$; (**b**) $k = 1$, $w = 10\,\text{m/s}$; (**c**) $k = 2$, $w = 0\,\text{m/s}$; (**d**) $k = 2$, $w = 10\,\text{m/s}$.

5.2.2. Eavesdropping Probability in AUSNs

Figure 10 shows the results of eavesdropping probability in AUSNs with an array eavesdropper ($M = 10$). Similarly, their transmission power can be calculated by Equation (15) and the reference transmission power of nodes is $P_t^i = 100$ dB. We can also see that the simulation results accurately match the analytical results. Besides, the eavesdropping probability increases with the increased node density ρ and decreases with the increased signal frequency f. Moreover, the eavesdropping probability decreases with increased wind speed w or spreading factor k. If we align Figures 9 and 10 together, we can find AUSNs have the lower eavesdropping probability than IUSNs, which implies that nodes have less chance of being eavesdropped upon in AUSNs than in IUSNs.

5.3. Comparison between an Isotropic Eavesdropper and an Array Eavesdropper

If we compare the eavesdropping probability of an isotropic eavesdropper with that of an array eavesdropper in AUSNs by aligning Figures 8 and 10 together, we can see that an array eavesdropper always has the higher eavesdropping probability than an isotropic eavesdropper in AUSNs. We have a similar result in the case by comparing Figures 7 and 9 in IUSNs.

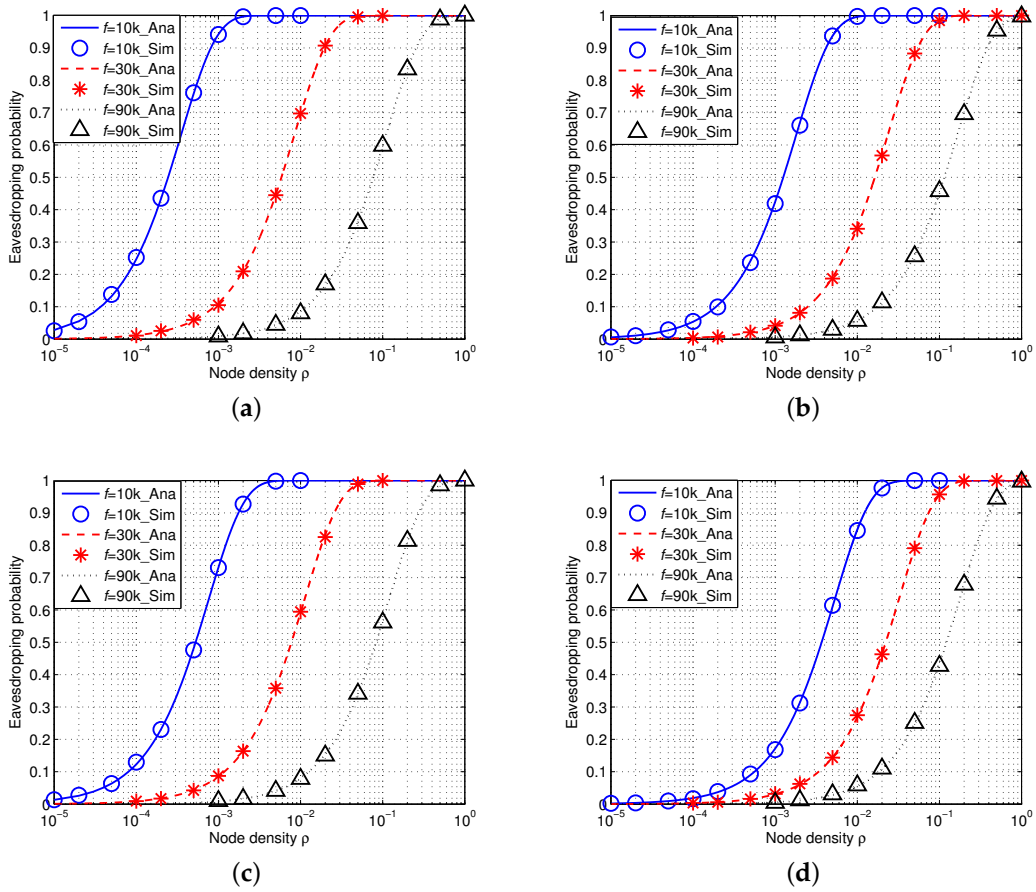

Figure 10. Eavesdropping probability in AUSNs with an *array* eavesdropper with different nodes density ρ ($/\mathrm{km}^2$) when $f = 10$ kHz, $f = 30$ kHz and $f = 90$ kHz under different spreading factor k and wind speed w. (**a**) $k = 1$, $w = 0\,\mathrm{m/s}$; (**b**) $k = 1$, $w = 10\,\mathrm{m/s}$; (**c**) $k = 2$, $w = 0\,\mathrm{m/s}$; (**d**) $k = 2$, $w = 10\,\mathrm{m/s}$.

6. Conclusions

In this paper, we propose an analytical model to investigate the eavesdropping probability in underwater acoustic sensor networks, which have different channel characteristics from those of terrestrial wireless sensor networks. In particular, we first establish the relationship between the eavesdropping probability and the underwater acoustic channel in both IUSNs and AUSNs considering an isotropic eavesdropper and an array eavesdropper, respectively. We then conduct extensive simulations to validate our model. The simulation results match our analytical results implying that our model is accurate and effective at analyzing the eavesdropping probability in underwater acoustic sensor networks. Besides, we also find that the eavesdropping probability heavily depends on signal frequency. Moreover, the results also show that the eavesdropping probability increases with the increased node density, decreases with the increased wind speed and decreases with the increased spreading factor. Comparing the eavesdropping probability in IUSNs with that in AUSNs, we find that equipping nodes with array line hydrophones can significantly decrease the eavesdropping probability of underwater acoustic sensor networks. One of the future research directions is to evaluate the effectiveness of our analytical model in realistic test-beds though it is challenging to implement underwater acoustic sensor networks (even with isotropic hydrophones) [41].

Acknowledgments: The work described in this paper was partially supported by Macao Science and Technology Development Fund under Grant No. 096/2013/A3 and the NSFC-Guangdong Joint Fund under Grant

No. U1401251. The authors would like to thank Gordon K.-T. Hon for his constructive comments. The authors would also like to thank the anonymous reviewers for their useful comments.

Author Contributions: Qiu Wang proposed the idea, derived the results and wrote the paper. Hong-Ning Dai supervised the work and revised versions. Xuran Li derive the initial results and contributed to the initial idea. Hao Wang gave valuable suggestions on the motivation of conducting analysis on eavesdropping attacks in underwater sensor networks and assisted in revising the paper. Hong Xiao contributed to revising and proofreading of the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Han, G.; Jiang, J.; Sun, N.; Shu, L. Secure communication for underwater acoustic sensor networks. *IEEE Commun. Mag.* **2015**, *53*, 54–60.
2. Baggeroer, A.B. Acoustic Telemetry-An Overview. *IEEE J. Ocean. Eng.* **1984**, *9*, 229–235.
3. Heidemann, J.; Stojanovic, M.; Zorzi, M. Underwater sensor networks: Applications, advances and challenges. *Philos. Trans. R. Soc. A* **2012**, *370*, 158–175.
4. Zhang, W.; Stojanovic, M.; Mitra, U. Analysis of a Linear Multihop Underwater Acoustic Network. *IEEE J. Ocean. Eng.* **2010**, *35*, 961–970.
5. Lucani, D.; Medard, M.; Stojanovic, M. Capacity scaling laws for underwater networks. In Proceedings of the 42nd Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, USA, 26–29 October 2008; pp. 2125–2129.
6. Shin, W.Y.; Lucani, D.E.; Médard, M.; Stojanovic, M.; Tarokh, V. On the Effects of Frequency Scaling over Capacity Scaling in Underwater Networks—Part I: Extended Network Model. *Wirel. Pers. Commun.* **2013**, *71*, 1683–1700.
7. Shin, W.Y.; Lucani, D.E.; Médard, M.; Stojanovic, M.; Tarokh, V. On the Effects of Frequency Scaling over Capacity Scaling in Underwater Networks—Part II: Dense Network Model. *Wirel. Pers. Commun.* **2013**, *71*, 1701–1719.
8. Watanabe, S.; Kamiya, Y.; Umebayashi, K.; Suzuki, Y. A New Efficient and Robust MAC Protocol against Multipath Fading for Ad Hoc Networks. In Proceedings of the 19th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'08), Cannes, France, 15–18 September 2008.
9. Mandal, P.; De, S. New Reservation Multiaccess Protocols for Underwater Wireless Ad Hoc Sensor Networks. *IEEE J. Ocean. Eng.* **2015**, *40*, 277–291.
10. Ahmed, S.; Javaid, N.; Khan, F.A.; Durrani, M.Y.; Ali, A.; Shaukat, A.; Sandhu, M.M.; Khan, Z.A.; Qasim, U. Co-UWSN: Cooperative Energy-Efficient Protocol for Underwater WSNs. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, doi:10.1155/2015/891410.
11. Pompili, D.; Melodia, T.; Akyildiz, I. Distributed Routing Algorithms for Underwater Acoustic Sensor Networks. *IEEE Trans. Wirel. Commun.* **2010**, *9*, 2934–2944.
12. Rahman, R.H.; Benson, C.; Frater, M. Routing Protocols for Underwater Ad Hoc Networks. In Proceedings of the 2012 IEEE Oceans, Yeosu, Korea, 21–24 May 2012 .
13. Javaid, N.; Jafri, M.R.; Ahmed, S.; Jamil, M.; Khan, Z.A.; Qasim, U.; Al-Saleh, S.S. Delay-Sensitive Routing Schemes for Underwater Acoustic Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, doi:10.1155/2015/532676.
14. Luo, Y.; Pu, L.; Zuba, M.; Peng, Z.; Cui, J.H. Challenges and Opportunities of Underwater Cognitive Acoustic Networks. *IEEE Trans. Emerg. Top. Comput.* **2014**, *2*, 198–211.
15. Ateniese, G.; Capossele, A.; Gjanci, P.; Petrioli, C.; Spaccini, D. SecFUN: Security Framework for Underwater acoustic sensor Networks. In Proceedings of the 2015 MTS/IEEE OCEANS, Genova, Italy, 18–21 May 2015.
16. Lu, X.; Yonghua, Z. Modeling the Wormhole Attack in Underwater Sensor Network. In Proceedings of the 12th IEEE International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–23 September 2012.
17. Zuba, M.; Shi, Z.; Peng, Z.; Cui, J.H.; Zhou, S. Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks. *Secur. Commun. Netw.* **2015**, *8*, 2635–2645.
18. Anjum, F.; Mouchtaris, P. *Security for Wireless Ad Hoc Networks*, 1st ed.; Wiley-Interscience: Hoboken, NJ, USA, 2007.
19. Wagner, D.; Schneier, B.; Kelsey, J. Cryptanalysis of the cellular message encryption algorithm. In *Advances in Cryptology—CRYPTO '97*; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1294, pp. 526–537.

20. IEEE 802.11a-1999. *Specifications: High Speed Physical Layer in the 5 GHz Band*; IEEE Standards Association: Piscataway, NJ, USA, 1999.
21. IEEE 802.11i-2004. *Amendment 6: Medium Access Control (MAC) Security Enhancements*; IEEE Standards Association: Piscataway, NJ, USA, 2004.
22. Granjal, J.; Monteiro, E.; Silva, J. Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294 – 1312.
23. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Comput. Netw.* **2008**, *52*, 2292–2330.
24. Kao, J.C.; Marculescu, R. Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks. In Proceedings of the IEEE 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, Reston, VA, USA, 28 September 2006; pp. 707–714.
25. Raymond, D.R.; Midkiff, S.F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Comput.* **2008**, *7*, 74–81.
26. Lu, X.; Wicker, F.; Lio, P.; Towsley, D. Security Estimation Model with Directional Antennas. In Proceedings of the 2008 IEEE Military Communications Conference, San Diego, CA, USA, 16–19 November 2008.
27. Dai, H.N.; Li, D.; Wong, R.C.W. Exploring Security Improvement of Wireless Networks with Directional Antennas. In Proceedings of the IEEE 36th Conference on Local Computer Networks (LCN), Bonn, Germany, 4–7 October 2011.
28. Wang, Q.; Dai, H.N.; Zhao, Q. Eavesdropping Security in Wireless Ad Hoc Networks with Directional Antennas. In Proceedings of the IEEE 2013 22nd Wireless and Optical Communication Conference, Chongqing, China, 16–18 May 2013; pp. 687–692.
29. Dai, H.N.; Wang, Q.; Li, D.; Wong, R.C.W. On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas. *Int. J. Distrib. Sens. Netw.* **2013**, *2013*, doi:10.1155/2013/760834.
30. Li, X.; Xu, J.; Dai, H.N.; Zhao, Q.; Cheang, C.F.; Wang, Q. On Modeling Eavesdropping Attacks in Wireless Networks. *J. Comput. Sci.* **2015**, *11*, 196–204.
31. Sankararaman, S.; Abu-Affash, K.; Efrat, A.; Eriksson-Bique, S.D.; Polishchuk, V.; Ramasubramanian, S.; Segal, M. Optimization Schemes for Protective Jamming. In Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, Hilton Head, SC, USA, 11–14 June 2012; pp. 65–74.
32. Kim, Y.S.; Tague, P.; Lee, H.; Kim, H. A Jamming Approach to Enhance Enterprise Wi-Fi Secrecy Through Spatial Access Control. *Wirel. Netw.* **2015**, *21*, 2631–2647.
33. He, X.; Khisti, A.; Yener, A. MIMO Multiple Access Channel With an Arbitrarily Varying Eavesdropper: Secrecy Degrees of Freedom. *IEEE Trans. Inf. Theory* **2013**, *59*, 4733–4745.
34. Zou, Y.; Champagne, B.; Zhu, W.P.; Hanzo, L. Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems. *IEEE Trans. Commun.* **2015**, *63*, 215–228.
35. Li, X.; Dai, H.N.; Zhao, Q. An Analytical Model on Eavesdropping Attacks in Wireless Networks. In Proceedings of the IEEE International Conference on Communication Systems (ICCS), Macau, 19–21 November 2014; pp. 538–542.
36. Emokpae, L.; Younis, M. Throughput Analysis for Shallow Water Communication Utilizing Directional Antennas. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 1006–1018.
37. Coates, R. *Underwater Acoustic Systems*; Palgrave Macmillan: London, UK, 1990.
38. Stojanovic, M. On the Relationship Between Capacity and Distance in an Underwater Acoustic Communication Channel. In Proceedings of the First ACM International Workshop on Underwater Networks (WUWNet), Los Angeles, CA, USA, 29 September 2006; pp. 41–47.
39. Hodges, R.P. *Underwater Acoustics: Analysis, Design and Performance of Sonars*, 1st ed.; Wiley: Hoboken, NJ, USA, 2010.
40. Bettstetter, C. On the Connectivity of Ad Hoc Networks. *Comput. J.* **2004**, *47*, 432–447.
41. Won, T.H.; Park, S.J. Design and Implementation of an Omni-Directional Underwater Acoustic Micro-Modem Based on a Low-Power Micro-Controller Unit. *Sensors* **2012**, *12*, 2309–2323.