

On Modeling of Eavesdropping Behavior in Underwater Acoustic Sensor Networks

Qiu Wang and Hong-Ning Dai

Macau University of Science and Technology, Macau SAR

Email: qiu_wang@foxmail.com and hndai@ieee.org

Abstract—In this paper, we propose a theoretical framework to investigate the eavesdropping behavior in underwater acoustic sensor networks. In particular, we quantify the eavesdropping activities by the eavesdropping probability. Our derived results show that the eavesdropping probability heavily depends on acoustic signal frequency, underwater acoustic channel characteristics (such as spreading factor and wind speed) and different hydrophones (such as isotropic hydrophones and array hydrophones). Simulation results have further validate the effectiveness and the accuracy of our proposed model.

Index Terms—Underwater; Acoustic Communication; Security; Eavesdropping

I. INTRODUCTION

Underwater Acoustic Sensor Networks (UASNs) are envisioned to enable a wide range of underwater applications for many scientific, commercial and military scenarios, such as ocean sampling, environmental monitoring, disaster prevention, assisted navigation, mine reconnaissance and distributed tactical surveillance [1]. UASNs often consist of heterogeneous power-limited sensors that are self-organised and deployed to perform collaborative work over a complex and fluctuating channel, which results in many security questions. For example, the high bit error rates resulting from the fluctuating channel in UASNs may cause the lost of critical packets. Consequently, confidential information can be eavesdropped, modified or dropped [2]. Besides, it is not feasible to apply computational-intensive encryption protocols for sensors with the limited power in UASNs.

The security of UASNs has recently received attention from academia. In particular, a cryptographic scheme was proposed to secure UASNs in [3] and a wormhole attack model was presented in [4]. But these models or schemes can not be used to model eavesdropping attacks, which one of typical security threats in UASNs. It is difficult to detect or prevent eavesdropping attacks since eavesdroppers only passively wiretap the transmissions without disclosing their existence. Moreover, many malicious attacks such as the man-in-the-middle attack [5], often go after wiretapping the information via eavesdropping attacks [6]. Therefore, it is necessary to quantify the eavesdropping attacks in UASNs. If we know better about eavesdroppers, we can design a better anti-eavesdropping mechanism [5], [7].

The main contributions of this paper are summarized as follows:

- we formally propose a theoretical model to quantify the eavesdropping behaviors in UASNs;

- we also take various underwater acoustic channel conditions (spreading factor and wind speed) into account;
- we consider two typical acoustic transceivers (isotropic hydrophones and array hydrophones) in UASNs and formally propose two types of UASNs depending on different transceivers equipped;
- we have conducted a number of simulations to evaluate the effectiveness and the accuracy of our proposed model.

II. UNDERWATER COMMUNICATION MODELS

As shown in previous studies [8], [9], [10], the underwater acoustic channel is typically affected by signal attenuation, ambient noise, etc. Firstly, the attenuation of acoustic signal in underwater environment in dB is given by the following equation,

$$10 \log A(d, f) = k \cdot 10 \log d + d \cdot 10 \log \alpha(f), \quad (1)$$

where d denotes the distance between a transmitter and receiver, k is spreading factor ($1 \leq k \leq 2$), and $10 \log \alpha(f)$ is absorption coefficient (dB/km) for acoustic signal frequency f (kHz), which is given by,

$$10 \log \alpha(f) = 0.11 \cdot \frac{f^2}{1 + f^2} + 44 \frac{f^2}{4100 + f^2} + 2.75 \cdot 10^{-4} f^2 + 0.003. \quad (2)$$

We then consider the ambient noise in UASNs, which is usually modeled by thermal noise, waves, turbulence and shipping activities. Particularly, the noise of waves is modeled by wind speed w (meter/second). The noise of shipping activities can be described by shipping activity factor s ($0 \leq s \leq 1$). Then, the formulae between power spectral density of total noise in dB re μ Pa per Hz and the acoustic signal frequency f in kHz are given by [9],

$$10 \log N(f) = 10 \log (N_t(f) + N_s(f) + N_w(f) + N_{th}(f)), \quad (3)$$

where $N_t(f)$ is the noise of turbulence and $10 \log N_t(f) = 17 - 30 \log(f)$, $N_s(f)$ is the noise of shipping activity and $10 \log N_s(f) = 40 + 20(s - 0.5) + 26 \log(f) - 60 \log(f + 0.03)$, $N_w(f)$ is the noise of wind and $10 \log N_w(f) = 50 + 7.5w^{1/2} + 20 \log(f) - 40 \log(f + 0.4)$, $N_{th}(f)$ is the noise of thermal, and $10 \log N_{th}(f) = -15 + 20 \log(f)$.

Next, we introduce hydrophones of UASNs. Hydrophones are used as receivers to collect acoustic signals in UASNs. Isotropic hydrophones are typically used in traditional UASNs

and they can receive signals uniformly in all direction. Differently, *array hydrophones* consisting of an array of isotropic hydrophones elements can effectively collect signals in certain directions.

In order to compare array hydrophones with isotropic hydrophones, we propose *Array Gain* (i.e., AG) in terms of the improved gain of signal-to-noise ratio (SNR) of array hydrophones over an isotropic hydrophone. Obviously, for an isotropic hydrophone, we have $AG = 1$. One of most common array hydrophones is an unshaded uniform linear array hydrophone, and the array gain $AG = M$ [10], where M is the number of isotropic hydrophone elements (due to the paper limitation, we omit the derivation). It implies that an array hydrophone can bring the M times SNR improvement in contrast to a single isotropic hydrophone.

III. ANALYSIS OF EAVESDROPPING BEHAVIOR IN UASNS

In this paper, we consider two kinds of UASNs: 1) each node is mounted with an isotropic hydrophone; we call such UASNs as IUSNs; 2) each node is mounted with an array hydrophone ($M = 10$); we call such UASNs as AUSNs. Besides, we assume that nodes follows a homogeneous Poisson point process with density ρ . Then, we consider an eavesdropper located in the center of UASNs, which equipped with an isotropic hydrophone since the eavesdropper has no knowledge of the location of nodes and an isotropic hydrophone can receive signal from all directions, as shown in Fig. 1.

To model the eavesdropping risk, we propose the *eavesdropping probability* (i.e., $\mathbb{P}(E)$). In particular, $\mathbb{P}(E)$ is the probability that any transmission can be wiretapped by a malicious node. We further investigate *effective eavesdropping area* denoted by D in order to quantify the number of the wiretapped transmissions. Take Fig. 1 as an example, where the effective eavesdropping area is bounded by a circle with radius $d_{\max}$. Note that $d_{\max}$ is the *maximum eavesdropping distance*, within which an eavesdropper can wiretap information successfully. It is obvious that $D = \pi d_{\max}^2$. Since nodes follow a homogeneous Poisson point process with density λ , we can obtain the *eavesdropping probability* $\mathbb{P}(E)$ as follows,

$$\mathbb{P}(E) = 1 - \mathbb{P}(Y = 0) = 1 - e^{-\lambda\pi(d_{\max})^2}, \quad (4)$$

where Y denotes the number of nodes in the effective eavesdropping area.

In order to calculate the maximum eavesdropping distance $d_{\max}$, we first consider link condition of UASNs. Let P_t denotes the transmission power. We then have SNR at receiver can be expressed as the following equation,

$$SNR = \frac{AG \cdot P_t}{\int_B A(d, f) df \int_B N(f) df}, \quad (5)$$

where $AG = 1$ in IUSNs and $AG = M$ in AUSNs, B is the bandwidth of underwater acoustic communications. Since we only concern with the connection between frequency SNR and f , we normalize the bandwidth. Eq. (5) can be converted

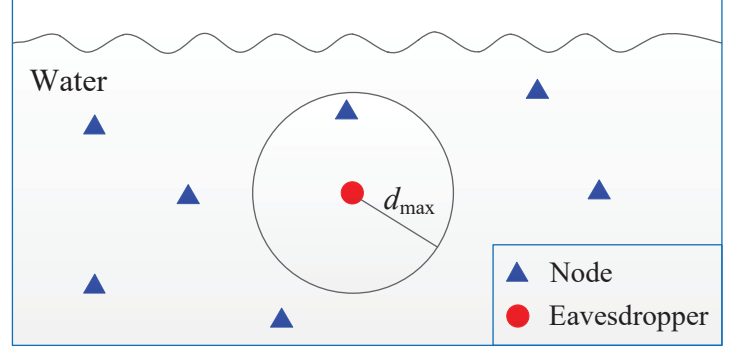


Fig. 1: Model of eavesdropping attack in UASNs

to

$$SNR = \frac{AG \cdot P_t}{A(d, f)N(f)}. \quad (6)$$

Eq. (6) can be expressed in dB as follows,

$$SNR_{dB} = 10 \log AG + 10 \log P_t - 10 \log A(d, f) - 10 \log N(f). \quad (7)$$

Generally, a link can be established if the signal-to-noise ratio SNR_{dB} is no less than a threshold δ_0 . If we let $SNR_{dB} = \delta_0$, we can have the minimum transmission power P_t (dB). In this paper, we assume that both AUSNs and IUSNs apply power control scheme to save power since power is limited in UASNs [2], which means that the nodes in AUSNs and IUSNs use the minimum transmission power. We let P_t^i denotes the minimum transmission power in IUSNs and P_t^a denotes the minimum transmission power in AUSNs. Then, the relationship between P_t^i and P_t^a can be calculated from Eq. (7) as follows,

$$10 \log P_t^a = 10 \log P_t^i - 10 \log M. \quad (8)$$

We next define the eavesdropping success condition. Essentially, the condition of successful wiretapping is equivalent to the condition of establishing a link. Thus, the eavesdropper can successfully wiretap information if and only if $SNR_{dB} \geq \delta_0$. Combining Eq. (7) and Eq. (1). We then have

$$k \cdot 10 \log d + d \cdot 10 \log \alpha(f) + 10 \log N(f) \leq 10 \log P_t - \delta_0. \quad (9)$$

We can see that left-hand-side (LHS) of Eq. (9) is an increasing function of the distance d . Therefore, we can get the maximum eavesdropping distance $d_{\max}$ if we let LHS of Eq. (9) be equal to right-hand-side (RHS). However, since Eq. (9) is a transcendental function of d , it is difficult to obtain a close form expression of $d_{\max}$. Thus, only the numerical results can be obtained as shown in our previous paper [10].

IV. SIMULATION RESULTS

In this section, results from computer simulations are given along with theoretical results in Section III. We conduct simulations on eavesdropping probability in both IUSNs and AUSNs with simulation tool MATLAB. In particular, we set the reference transmission power $P_t^i = 100\text{dB}$, node density

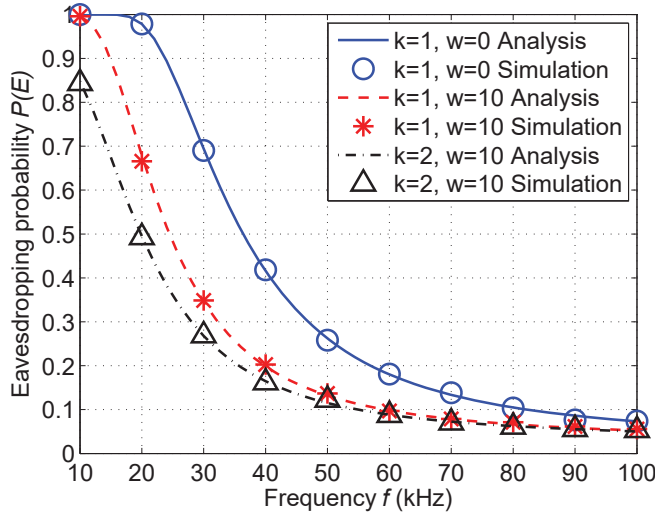


Fig. 2: Eavesdropping probability $\mathbb{P}(E)$ of IUSNs.

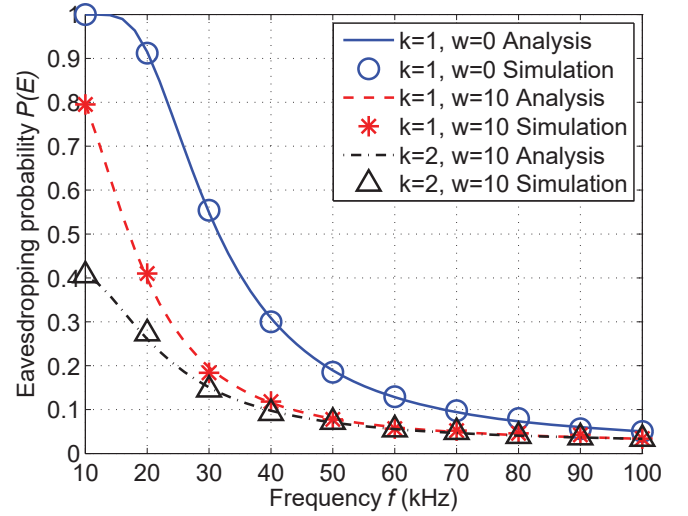


Fig. 3: Eavesdropping probability $\mathbb{P}(E)$ of AUSNs.

$\lambda = 0.01$, the signal-to-noise threshold $\delta_0 = 20\text{dB}$ and shipping activity factor $s = 1$.

Fig. 2 and Fig. 3 show the analysis and simulation results of eavesdropping probability in IUSNs and in AUSNs, respectively. In particular, we plot the analytical results as curves and present the simulations results as markers. Note that each simulation data point is the averaged value over 5000 random topologies.

We can see that simulation results agree with the analytical results, implying that our presented analytical framework is accurate. Besides, from both Fig. 2 and Fig. 3, we can see that the eavesdropping probability is significantly affected by acoustic signal frequency f and underwater channel characteristics. In particular, $\mathbb{P}(E)$ decreases with the increased frequency f , decreases with increased w and decreases with increased k . Moreover, in contrast to IUSNs, AUSNs can decrease the eavesdropping probability. This can be verified by comparing the results of IUSNs and AUSNs together (by aligning Fig. 2 with Fig. 3). This finding implies that we can deploy array hydrophones to UASNs to decrease the eavesdropping risk.

V. CONCLUSION

This paper has presented a framework for eavesdropping in underwater acoustic sensor networks analysis, where the channel characteristics are totally different from terrestrial wireless sensor networks. In particular, this framework provides a relationship between the eavesdropping probability and the underwater acoustic channel in both IUSNs and AUSNs. The extensive simulations has validated the accuracy of this framework. Results show that eavesdropping probability significantly depends on acoustic signal frequency. Besides, eavesdropping probability decreases with the increased wind speed and decreases with the increased spreading factor. We also find that equipping nodes with array hydrophones in

networks (AUSNs) can significantly decrease the eavesdropping probability than equipping with isotropic hydrophones in networks (IUSNs).

ACKNOWLEDGEMENT

The work described in this paper was supported by Macao Science and Technology Development Fund under Grant No. 096/2013/A3. The authors would like to thank anonymous reviewers for their constructive comments. The authors would like to express their appreciation for Gordon K.-T. Hon for his thoughtful discussions.

REFERENCES

- [1] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: Research challenges," *AD HOC NETWORKS*, vol. 3, pp. 257–279, 2005.
- [2] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Communication*, pp. 22–28, February 2011.
- [3] G. Ateniese, A. Caposelle, P. Gjanci, C. Petrioli, and D. Spaccini, "Secfun: Security framework for underwater acoustic sensor networks," in *Proceedings of OCEANS - Genova, 2015 MTS/IEEE*, May 2015.
- [4] X. Lu and Z. Yonghua, "Modeling the wormhole attack in underwater sensor network," in *Proceedings of the 12th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE*, 2012.
- [5] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215 – 228, 2015.
- [6] F. Anjum and P. Mouchtaris, *Security for Wireless Ad Hoc Networks*, 1st ed. Wiley-Interscience, 2007.
- [7] X. He, A. Khisti, and A. Yener, "MIMO Multiple Access Channel With an Arbitrarily Varying Eavesdropper: Secrecy Degrees of Freedom," *IEEE Transactions on Information Theory*, pp. 4733–4745, Aug. 2013.
- [8] R. Coates, *Underwater Acoustic Systems*. Palgrave Macmillan, 1990.
- [9] M. Stojanovic, "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)*, 2006, pp. 41 – 47.
- [10] Q. Wang, H.-N. Dai, X. Li, H. Wang, and H. Xiao, "On Modeling Eavesdropping Attacks in Underwater Acoustic Sensor Networks," *Sensors*, vol. 16, no. 5, p. 721, 2016.