2016 IEEE International Conference on Computational Science and Engineering, IEEE International Conference on Embedded and Ubiquitous Computing, and International Symposium on Distributed Computing and Applications to Business, Engineering and Science

On Eavesdropping Attacks in Wireless Networks

Hong-Ning Dai*, Hao Wang†, Hong Xiao‡, Xuran Li* and Qiu Wang*
*Macau University of Science and Technology, Macau SAR
†Norwegian University of Science and Technology, Aalesund, Norway
‡Faculty of Computer, Guangdong University of Technology, Guangzhou, China

***Abstract*—Eavesdropping attacks have become one of major threats in wireless networks since it is the prerequisite of other malicious attacks. Most of current studies concentrate on designing anti-eavesdropping schemes. There are few studies on quantitatively evaluating the eavesdropping attacks conducted by the malicious nodes. However, it is important to investigate the eavesdropping attacks since we can design cost-effective anti-eavesdropping schemes if we know the eavesdropping behaviors. For example, we can offer a better protection on the confidential communications if we know which location is more vulnerable to eavesdropping attacks. In this paper, we propose a general analytical framework to quantify the eavesdropping probability in wireless networks with consideration of various factors, such as node density and impacts of channel conditions. We validate the accuracy of our proposed model by conducting extensive simulations. Besides, we show that our general model can also be used to underwater acoustic networks.**

I. Introduction

These security issues in wireless networks are significantly different from those in conventional wired networks due to the following inherent constraints of wireless networks [1]: (i) the wireless medium is open for any nodes; (ii) wireless networks consist of a number of autonomous nodes that are free to join and leave the networks; (iii) it is also difficult to implement the centralized security countermeasures in *distributed* wireless networks [2]. In wireless networks, any wireless user residing in the *transmission* range of the transmitter can potentially decode the signal while both the transmitter and the receiver are unaware of the *reconnaissance* (or *eavesdropping* activity) [3]. Consider the scenario as shown in Fig. 1, where there are two wireless users Alice and Bob communicating with each other and the eavesdropper Eve is wiretapping the transmission between Alice and Bob. Specifically, there are two types of eavesdropping attacks in wireless networks [4]: (i) *Passive Eavesdropping*, in which the *malicious* nodes detect the information by listening to the message transmission in the broadcasting wireless medium; (ii) *Active Eavesdropping*, where the malicious nodes actively grab the information via sending queries to transmitters by disguising themselves as friendly nodes. The study on the passive eavesdropping attacks is more challenging than that on the active eavesdropping attacks since it is more difficulty to detect passive eavesdroppers (as they seldom expose their existence). Besides, it is more important to analyze the passive eavesdropping attacks because the malicious nodes must have the knowledge of the friendly nodes via conducting passive eavesdropping activities before they can actively attack the friendly nodes. Therefore, our study in this paper is mainly concentrated on the passive eavesdropping attacks.

Most of current studies are concentrated on the encryption of the confidential communications in wireless networks [5]. However, encryption algorithms may not be feasible to wireless networks due to (a) the inferior computational capability of wireless nodes, especially for wireless sensor nodes or smart objects in IoT [2], (b) the limited battery power of wireless nodes (e.g., the passive RFIDs have no energy supply an can only harvest the energy from the readers) [6], and (c) the difficulty of managing the widely distributed nodes in centralized manner, which is the necessity for the encryption algorithms [5]. An alternate approach is either to design light-weighted encryption schemes [7] or to generate noise to limit the amount of information that can be extracted by an *eavesdropper* [8]. However, all above schemes require that we shall have enough knowledge of the channel condition of eavesdroppers as indicated in [9], [10], which nevertheless has received little attention.

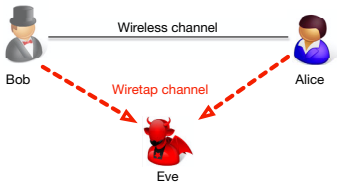


Fig. 1. Eavesdropping activity

Therefore, the main purpose of this paper is to investigate the eavesdropping attacks in wireless networks. In particular, we propose a general analytical framework to quantitatively evaluate the eavesdropping probability in wireless networks. Our analytical model has the following merits: (i) *Generality*. Our analytical model considers various channel conditions (path loss, shadowing, multi-path effects, etc.); (ii) *Pervasiveness*. Our analytical model can be used to analyze both *terrestrial* wireless networks and *underwater acoustic* networks; (iii) *Accuracy*. Our model can accurately analyze the eavesdropping probability. In particular, extensive simulation results validate the accuracy of our model.

The remaining paper is organized as follows. We first present the system model in Section II. Section III then presents the analysis of eavesdropping attacks with consideration of various channel conditions. Finally, the paper is concluded in Section IV.

II. System Model

A. Terrestrial wireless channel model

In this paper, we assume all the wireless users (or nodes) are randomly distributed in a 2-D plane with area $\mathcal{A}$ according to a homogeneous Poisson point process (PPP) with density

978-1-5090-3593-9/16 $31.00 © 2016 IEEE
DOI 10.1109/CSE-EUC-DCABES.2016.173

ρ. We denote the number of nodes in an area $\mathcal{A}$ by a random variable N. Then, the probability mass function of N is given as $f_N(n) = \frac{(\rho\mathcal{A})^n}{n!}e^{-\rho\mathcal{A}}$. Besides, we assume that all nodes use the common transmission power $\mathcal{P}_t$. We denote the channel gain from a node i to an eavesdropper j at a distance r by $\gamma_{ij}(r)$. Thus, the received power at the eavesdropper is $\mathcal{P}_t \cdot \gamma_{ij}(r)$. The signal-to-noise ratio (SNR) at the eavesdropper denoted by Λ is defined to be

$$\Lambda = \frac{\mathcal{P}_t \cdot \gamma_{ij}(r)}{\eta}, \tag{1}$$

where η is the power of the white noise and N denoted the number of good nodes. We then have the eavesdropping criteria in the general case.

Definition 1: Eavesdropping Criteria. The transmission from node i can be successfully eavesdropped by an eavesdropper if and only if $\Lambda \geq \beta$, where β is the minimum signal to noise ratio.

In this paper, we do not consider the impact of interference in this paper because (i) the passive eavesdroppers do not transmit actively and therefore contribute nothing to the interference; (ii) the interference contributed by other nodes is proved to converge when efficient MAC schemes are exploited and the traffic is low in a large scale network [11], [12]. We will investigate the impact of interference in our future study. We then have

$$\Lambda = \frac{\mathcal{P}_t \cdot \gamma_{ij}(r)}{\eta} \geq \beta. \tag{2}$$

B. Underwater acoustic channel

Due to the high attenuation of electromagnetic waves in underwater environments, acoustic communications are typically used in underwater networks. Underwater acoustic communication channel is characterized by a path loss that depends on not only the distance between the transmitter and the receiver, but also the signal frequency. In particular, the path loss or the attenuation that occurs in an underwater acoustic channel over a distance r for a signal of frequency f is given by the following equation [13],

$$A(r, f) = r^k \alpha(f)^r, \tag{3}$$

where k is the spreading factor (ranging from 1 to 2) and $\alpha(f)$ is the absorption coefficient of signal frequency f. Usually, Eq. (3) can be expressed in dB as follows

$$10\log A(r, f) = k \cdot 10\log r + d \cdot 10\log\alpha(f). \tag{4}$$

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 $10\log\alpha(f) = 0.11 \cdot \frac{f^2}{1+f^2} + 44\frac{f^2}{4100+f^2} + 2.75\cdot 10^{-4} f^2 + 0.003$. For the lower frequency f, we have the absorption coefficient $10\log\alpha(f)$ as $10\log\alpha(f) = 0.002 + 0.11\frac{f^2}{1+f^2} + 0.011 f^2$.

III. Analysis of Eavesdropping Attacks

A. Impacts of Path Loss Effect

We first consider the impact of path loss effect on the channel gain $\gamma_{ij}(r)$, which is given by

$$\gamma_{ij}(r) = k_1 \cdot G_g \cdot G_e \cdot \frac{1}{r^\alpha}, \tag{5}$$

where k_1 is a constant, r is the distance between the normal user and the eavesdropper, G_g and G_e are the antenna gains for the normal user and the eavesdropper, respectively, and α is the path loss exponent ranging from 2 to 4 [14].

As shown in Section II-A, an eavesdropper can successfully wiretap a transmission if and only if its $\Lambda \geq \beta$. In other words, the probability of no transmission eavesdropped is given by $\mathbb{P}(\Lambda < \beta)$. Substituting Eq. (5) into inequality (2) and rearranging $P(\Lambda < \beta)$, we have

$$\mathbb{P}(\Lambda < \beta) = \mathbb{P}\left(\frac{\mathcal{P}_t \cdot k_1 \cdot G_g \cdot G_e}{\eta \cdot r^\alpha} < \beta\right) = \mathbb{P}\left(r > \left(\frac{\mathcal{P}_t \cdot k_1 \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{\frac{1}{\alpha}}\right). \tag{6}$$

We then define the *eavesdropping range* denoted by a random variable R as

$$R = \left(\frac{\mathcal{P}_t \cdot k_1 \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{\frac{1}{\alpha}}. \tag{7}$$

After substituting Eq. (7) into inequality part of Eq. (6), we have $\mathbb{P}(\Lambda < \beta) = P(r > R)$, which implies that a transmission cannot be eavesdropped by an eavesdropper if and only if the transmitter falls outside the eavesdropping range R of the eavesdropper. We then analyze the *effective eavesdropping area* of an eavesdropper, which is defined as $\mathbb{E}[\pi R^2] = \pi\mathbb{E}[R^2]$, where $\mathbb{E}[R^2]$ is the second moment of the eavesdropping range R. The effective eavesdropping area is a *critical* region, in which its transmission can be eavesdropped by eavesdroppers only when the good node falls in this region. We then have

$$\mathbb{E}[\pi R^2] = \pi\mathbb{E}\left[\left(\frac{k_1 \cdot \mathcal{P}_t \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{\frac{2}{\alpha}}\right]. \tag{8}$$

We model the successful chance of eavesdropping attacks by the *probability of eavesdropping attacks*, denoted by $\mathbb{P}(E)$. We denote the number of good nodes falling in the eavesdropping area by a random variable Y. Since good nodes are randomly distributed according to a homogeneous PPP, we then have the probability of no good node falling in the eavesdropping area, which is given by $\mathbb{P}(Y = 0) = e^{-\rho\cdot\mathbb{E}[\pi R^2]}$.

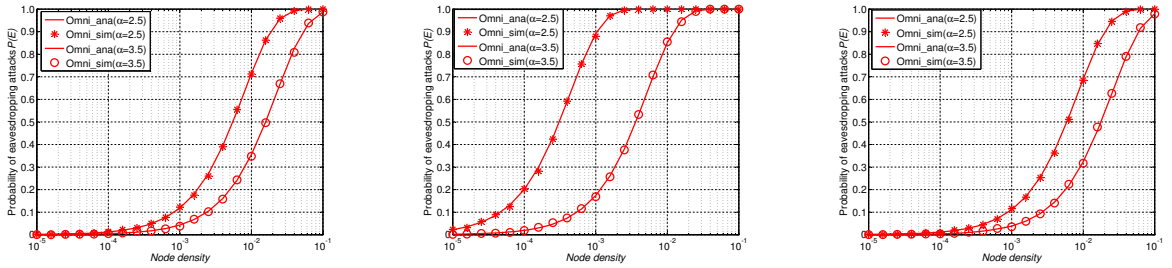
We then can calculate $\mathbb{P}(E)$ as follows,

$$\mathbb{P}(E) = 1 - \mathbb{P}(Y = 0) = 1 - e^{-\rho\cdot\mathbb{E}[\pi R^2]}. \tag{9}$$

After substituting $\mathbb{E}[\pi R^2]$ in Eq. (9) by RHS of Eq. (8), we have

$$\mathbb{P}(E) = 1 - \exp\left(-\rho\cdot\pi\mathbb{E}\left[\left(\frac{k_1 \cdot \mathcal{P}_t \cdot G_g \cdot G_e}{\eta \cdot \beta}\right)^{\frac{2}{\alpha}}\right]\right). \tag{10}$$

The physical meaning of $\mathbb{P}(E)$ is the probability that an eavesdropper can successfully eavesdrop at least one transmission in wireless network. Besides, as shown in Eq. (10), the probability of eavesdropping attacks heavily depends on the path loss effect. Note that this model can be extended to more general cases with consideration of the shadow fading effect and the Rayleigh fading effect, which will be analyzed next.



(a) Path loss effect only (b) Shadowing effect when $\sigma = 3$ (c) Rayleigh fading without shadowing effect

Fig. 2. Probability of eavesdropping attacks $\mathbb{P}(E)$ in terrestrial wireless networks with impacts of various channel effects where SINR threshold $\beta = 10$dB

B. Impacts of Shadowing Effect

Following the similar approach as described in our previous work [15], we can derive the probability density function (PDF) of R with consideration of the shadow fading effect as follows,

$$\mathbb{P}(E) = 1 - \exp\left(-\rho\pi\left(\frac{\mathcal{P}_t A_G k_1}{\eta\beta}\right)^{\frac{2}{\alpha}} \exp\left(\frac{\sqrt{2}\sigma}{\alpha}\right)^2\right). \quad (11)$$

The probability of eavesdropping attacks in Eq. (11) is more general than that in Eq. (10). This is because Eq. (11) becomes Eq. (10) when σ becomes 0, implying that there is no shadow fading effect and SINR is completely determined by the path loss effect.

C. Impacts of Rayleigh Fading Effect

Rayleigh fading effect is a stochastic model for wireless propagation when there are a large number of statistically independent reflected and scattered paths from the transmitters to the receivers (or the eavesdroppers). To model such fading effect is non-trivial and involved with many theoretical techniques [12], [16]. Due to the space limitation, we only give the final derived equation (the detailed derivation can be found in [15]). The eavesdropping probability under Rayleigh fading channel is

$$\mathbb{P}(E) = 1 - e^{-\rho\pi\frac{2}{\alpha}\Gamma(\frac{2}{\alpha})\cdot(\frac{\eta\cdot\beta}{k_1\cdot\mathcal{P}_t\cdot A_G})^{-\frac{2}{\alpha}}\cdot e^{(\frac{\sqrt{2}\sigma}{\alpha})^2}}. \quad (12)$$

D. Simulation Validation

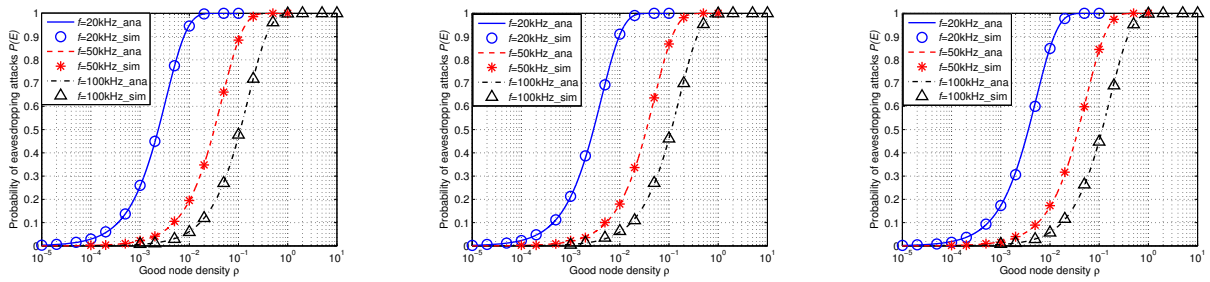
In our simulations, the probability of eavesdropping attacks is calculated by $\mathbb{P}_s(E) = \frac{\psi}{\Psi}$, where Ψ denotes the number of total network topologies and ψ represents the number of network topologies that have been eavesdropped. Here, we denote the simulation results by $\mathbb{P}_s(E)$ in order to differentiate it from the analytical value $\mathbb{P}(E)$.

We plot the analytical results and the simulation results of the probability of eavesdropping attacks with the path loss effect only in Fig. 2(a), where the curves and the markers represent the analytical results and simulation results, respectively. It is obvious that the simulation results well agree with the analytical results, implying that our model is quite accurate. Besides, Fig. 2(a) also indicates that the probability of eavesdropping attacks decreases with the increased path loss exponent α, implying that the path loss effect has the negative impact on eavesdropping attacks. Fig. 2(b) shows the results of the probability of eavesdropping attacks with consideration of shadowing effect, where the shadowing deviation $\sigma = 3$. Similarly, it is shown in Fig. 2(b) that the simulation results match with the analytical results, implying the accuracy of our model. Besides, Fig. 2(b) indicates that the probability of eavesdropping attacks is affected by both the path loss effect and the shadowing effect. In particular, $\mathbb{P}(E)$ decreases with the increased path loss exponent α, implying that the path loss effect is *detrimental*. On the contrary, the shadowing effect is *beneficial*. More specifically, if we align Fig. 2(b) with Fig. 2(a), we can find that $\mathbb{P}(E)$ increases with the increased values of the shadowing deviation σ (e.g., σ is increased from 0 to 3). This effect is remarkable when the path loss effect is less notable (e.g., $\alpha = 2.5$). However, $\mathbb{P}(E)$ does not increase significantly with the increased values of σ when $\alpha = 3.5$. Fig. 2(c) shows the empirical results of the probability of eavesdropping attacks under the channel with Rayleigh fading effect only, where $\sigma = 0$ indicating no shadowing effect. It is shown in Fig. 2(c) that the simulation results have a good agreement with the analytical results, implying that our analytical model is quite accurate. Besides, it is shown in Fig. 2(c) that the probability of eavesdropping attacks also depends on both the path loss effect and Rayleigh fading effect. In particular, $\mathbb{P}(E)$ drops significantly when the path loss effect becomes more notable (e.g., $\alpha = 3.5$), as shown in Fig. 2(c). Besides, under the channel with Rayleigh fading effect, $\mathbb{P}(E)$ in Fig. 2(c) is even lower than that without Rayleigh fading effect in Fig. 2(a), implying that Rayleigh fading effect is also *detrimental* to the eavesdropping attacks. The reason may owe to the counteracting effect of the multi-path scattering signals with Rayleigh fading effect [14].

E. Extension to Underwater Acoustic Networks

Our proposed model can also be used to evaluate the eavesdropping probability in underwater acoustic networks [17]. It is worth to mention that the underwater acoustic communication channel has the different features from that of terrestrial wireless channel as shown in Section II-B. We then conduct 3 sets of simulations, each of which is obtained by choosing different values of spreading factor k (i.e., $k = 1$, $k = 1.5$ and $k = 2$), respectively. Specifically, we set the acoustic signal frequency f with 20kHz, 50kHz and 100kHz, respectively for each set of the simulations. Note that we fix the threshold attenuation $\beta_0 = 50$dB in all the three sets of simulations. Fig. 3 plot the results.

Fig. 3(a) shows the first set of simulation results with spreading factor $k = 1$. We can see that there is an excellent



(a) Spreading factor $k = 1$ (b) Spreading factor $k = 1.5$ (c) Spreading factor $k = 2$

Fig. 3. Probability of eavesdropping attacks $\mathbb{P}(E)$ in underwater acoustic networks with different node density ρ (/km^2) when $f = 20$kHz, $f = 50$kHz and $f = 100$kHz

agreement of the simulation results with the analytical results. This indicates that our proposed analytical model is accurate. Besides, the eavesdropping probability increases with the node density ρ. Moreover, if we compare three different curves of frequency f (the blue one, the red one, the black one) together in Fig. 3(a), we can find that $\mathbb{P}(E)$ decreases with the increased frequency f. This is because the acoustic signal attenuation goes much faster when the frequency of the acoustic signal is increased in underwater environment. As a result, the eavesdropping probability also decreases.

Fig. 3(b) and Fig. 3(c) show the second set of simulations and the third set of simulations with spreading factor $k = 1.5$ and $k = 2$, respectively. Observed from these two sets of results, we can also draw a conclusion that our analytical model is accurate to model the eavesdropping probability in underwater acoustic networks since the simulation results match the analytical results. Similarly, we can also see that the eavesdropping probability increases with the increased good node density and decreases with the increased signal frequency. If we put Fig. 3(a), Fig. 3(b) and Fig. 3(c) together, we can find that the values of $\mathbb{P}(E)$ decreases as spreading factor k increases. For example, if we draw three vertical lines in Fig. 3(a), Fig. 3(b) and Fig. 3(c) with the fixed node density $\rho = 0.02$ and choose the curves with the same signal frequency $f = 50$kHz in each of the above figures, we can obtain the values of $\mathbb{P}(E)$, which are equal to 0.359, 0.329, 0.308 with $k = 1$, $k = 1.5$ and $k = 2$, respectively.

IV. Conclusion

In this paper, we investigate the eavesdropping attacks in wireless networks. Specifically, we propose a general model to quantitatively evaluate the eavesdropping risk in wireless networks. Our model considers various channel conditions such as path loss, shadowing and multi-path fading effects. Besides, our model can also be applied to both terrestrial wireless networks and underwater acoustic networks. Extensive simulation results also validate the accuracy of our model.

Acknowledgment

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.

References

[1] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When Does Relay Transmission Give a More Secure Connection in Wireless Ad Hoc Networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 624 – 632, 2014.

[2] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497 – 1516, 2012.

[3] F. Anjum and P. Mouchtaris, *Security for Wireless Ad Hoc Networks*, 1st ed. Wiley-Interscience, 2007.

[4] M. Anand, Z. G. Ivesy, and I. Leez, "Quantifying eavesdropping vulnerability in sensor networks," in *Proceedings of the 2nd International VLDB Workshop on Data Management for Sensor Networks*, 2005.

[5] J. Granjal, E. Monteiro, and J. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294 – 1312, 2015.

[6] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd Annual Design Automation Conference (DAC)*, 2015.

[7] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks." in *ACM Conference on Computer and Communications Security*, 2007.

[8] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, and J. Reverdy, "RFID Noisy Reader How to Prevent from Eavesdropping on the Communication?" in *Cryptographic Hardware and Embedded Systems - CHES*, ser. Lecture Notes in Computer Science, vol. 4727, 2007, pp. 334–345.

[9] 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.

[10] 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.

[11] M. Francheschetti, O. Dousse, D. Tse, and P. Thiran, "Closing the gap in the capacity of random wireless networks via percolation theory," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1009–1018, 2007.

[12] D. Miorandi, E. Altman, and G. Alfano, "The Impact of Channel Randomness on Coverage and Connectivity of Ad Hoc and Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 1062 – 1072, 2008.

[13] R. Coates, *Underwater Acoustic Systems*. Palgrave Macmillan, 1990.

[14] T. S. Rappaport, *Wireless communications : principles and practice*, 2nd ed. Upper Saddle River, N.J.: Prentice Hall PTR, 2002.

[15] X. Li, H. Wang, H.-N. Dai, Y. Wang, and Q. Zhao, "An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things," *Mobile Information Systems*, vol. 2016, 2016.

[16] J. G. Proakis, *Digital Communications*, 4th ed. McGrawHill, 2001.

[17] Q. Wang, H.-N. Dai, X. Li, H. Wang, and H. Xiao, "On Modeling Eavesdropping Attacks in Underwater Acoustic Sensor Networks," *Sensors*, 2016.