Physical Layer Security With Uncertainty on the Location of the Eavesdropper

Dimitrios S. Karas, *Student Member, IEEE*, Alexandros–Apostolos A. Boulogeorgos, *Student Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—We investigate the physical layer (PHY) security of a system with a base-station (BS), a legitimate user, and an eavesdropper, whose exact location is unknown but within a ring-shaped area around the BS. To this end, we present novel closed-form expressions for the secrecy outage probability, which take into consideration both the impact of fading, as well as the eavesdropper's location uncertainty. The derived expressions are validated through simulations, which reveal that the level of uncertainty should be seriously taken into account in the design and deployment of a wireless system with PHY security.**

***Index Terms*—Performance analysis, secrecy capacity, secrecy outage probability.**

I. Introduction

PHYSICAL layer (PHY) security has received significant attention in the last years, since it can provide reliable and secure communication by employing the fundamental characteristics of the transmission medium, such as multipath fading [1]. Until recently, the locations of the legitimate user and the eavesdropper were assumed to be known to the base-station (BS) (see [2]–[4] and references therein).

However, this assumption was questioned in [5]–[12], since in the case of a purely passive eavesdropper, its location is not realistic to be known to the BS [5]. Specifically, in [5], the probability for non-zero secrecy capacity was derived, assuming that the eavesdroppers were scattered according to a Poisson point process (PPP), while the BS has available instantaneous channel state information (CSI) of the legitimate user. In [6], the secrecy outage probability (SOP) was evaluated for a scenario where multiple colluding eavesdroppers are distributed according to a PPP, but the effect of multipath fading was not taken into consideration, and the derived expressions are not generally in closed-form. In [7], multiple BSs distrubuted according to a PPP are considered, but the authors assume full or partial knowledge of the location of the potential eavesdroppers. Also, the effect of fading was not taken into consideration, and the achievable secret transmission rate is presented in the form of bounds and approximations. In [8], the impact of uncertainty on Eve's location is investigated, but the CSI of the main channel is known to Alice, and the expression for the SOP is not closed-form, but it is given in a form of an infinite series. In [9] and [10], the uncertainty in Eve's location is handled by performing estimation with techniques, such as received signal strength, angle of arrival and time difference of arrival. In our work, we consider the case, where the hardware required for these techniques is not available to Alice. Furthermore, in [11], the location uncertainty was modeled in terms of node and link failures by using secrecy graphs. Finally, in [12], the authors considered a multiple BS scenario, in which the locations of the legitimate users and the eavesdroppers were assumed known, while the location of each BS was assumed unknown and modeled as a PPP.

In this work, we present closed-form expressions for the SOP, as a function of the targeted transmission rate, assuming that the eavesdropper's location is modeled as a uniform distribution over a ring-shaped area, centered at the BS's location. We also consider that the BS has available statistical CSI knowledge, for both the legitimate user and the eavesdropper. The derived expressions hold for any given path loss exponent, and they can be used in various practical scenarios to select deployment specifications, such as the targeted data rate and the minimum level of uncertainty that is required, in order to employ PHY security in a wireless system. To the best of the authors' knowledge, the impact of the uncertainty on the location of the eavesdropper in PHY security under these assumptions has not been addressed yet in the open technical literature.

II. System Model

We consider the downlink scenario in a wireless network that consists of a BS, which aims to transmit a confidential message to a legitimate user, in the presence of an eavesdropper. For convenience, we refer to the BS as Alice (A), the legitimate user as Bob (B), and the eavesdropper as Eve (E). The baseband equivalent signals received by Bob and Eve can be respectively written as

$$y_B = h_B x + n_B \text{ and } y_E = h_E x + n_E, \tag{1}$$

where x denotes the transmitted signal, n_B and n_E are zero mean complex Gaussian random variables (RVs) that represent zero-mean symmetric additive white Gaussian noises (AWGN), with power spectral density N_0 at Bob and Eve, respectively. Without loss of generality, we assume that the variance of the noise at Bob's and Eve's RXs is the same. Moreover, the channel between Alice and Bob is denoted by h_B, while that between Alice and Eve by h_E. Due to the distance, d_X, between Alice and node X, the channel gain can

Manuscript received July 19, 2016; accepted August 10, 2016. Date of publication August 15, 2016; date of current version October 11, 2016. The associate editor coordinating the review of this paper and approving it for publication was S. Gezici.

The authors are with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece (e-mail: dkaras@auth.gr; ampoulog@auth.gr; geokarag@auth.gr).

Digital Object Identifier 10.1109/LWC.2016.2600323

be expressed as in [13], and is given by

$$h_{\mathcal{X}} = \frac{g_{\mathcal{X}}}{\sqrt{1+d_{\mathcal{X}}^{\alpha}}}, \tag{2}$$

where $\mathcal{X} \in \{B, E\}$, while $|g_{\mathcal{X}}|$ and α denote the Rayleigh fading channel gain and the path loss coefficient, respectively. We assume that the distance between Alice and Bob is constant and known to Alice, while the exact distance between Alice and Eve is unknown to Alice. Furthermore, Eve's location is uniformly distributed in a ring centered at Alice's position, with inner radius R_1 and outer radius R_2. R_2 represents the BS's coverage region, since Eve has to be located at a position where she can reliably receive the signal transmitted by Alice. For a fixed R_2, R_1 shows the minimum distance between Alice and Eve required to achieve a target SOP, for the design and deployment of a system with specific SOP requirements. This is a realistic assumption, when Eve is not a legitimate member of the network. In practice, R_1 represents a secure region around the BS.

By using (2), the instantaneous signal-to-noise ratio (SNR) at Bob and Eve can be expressed as

$$\gamma_{\mathcal{X}} = \frac{|h_{\mathcal{X}}|^2 E_s}{N_0} = \frac{|g_{\mathcal{X}}|^2 E_s}{\left(1+d_{\mathcal{X}}^{\alpha}\right)N_0}, \tag{3}$$

where, E_s, represents the energy of the transmitted signal.

III. Secrecy Outage Probability

The secrecy capacity is given by [14]

$$C_s = \begin{cases} C_B - C_E, & C_B \geq C_E \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

where, $C_B = \log_2(\gamma_B + 1)$, is the capacity of the legitimate channel between Alice and Bob, and, $C_E = \log_2(\gamma_E + 1)$, is the capacity of the eavesdropper channel between Alice and Eve.

Proposition 1: The probability density function (PDF) of $|h_E|^2$ as given by (2) can be expressed as in (5), as shown at the bottom of the next page, while the cumulative distribution function (CDF) of $|h_E|^2$ can be obtained as

$$F_{|h_E|^2}(x) = 1 - 2\frac{R_1^2 E_{\frac{\alpha-2}{\alpha}}\left(R_1^{\alpha}x\right) - R_2^2 E_{\frac{\alpha-2}{\alpha}}\left(R_2^{\alpha}x\right)}{\left(R_2^2 - R_1^2\right)\alpha}\exp(-x), \tag{6}$$

where $E_n(\cdot)$ is the exponential integral function [15, Eq. (5.1.4)].

Proof: Please refer to Appendix A. ∎

The SOP is the probability that the secrecy capacity is lower than a target secrecy rate r_s, i.e., $P_o(r_s) = P_r(C_s \leq r_s)$, or equivalently

$$P_o(r_s) = P_r\left(\log_2\left(\frac{\gamma_B+1}{\gamma_E+1}\right) \leq r_s\right). \tag{7}$$

Theorem 1: The SOP can be expressed in closed-form as

$$P_o(r_s) = 1 - \exp\left[-\frac{\left(1+d_B^{\alpha}\right)(2^{r_s}-1)N_0}{E_s}\right] + L(r_s), \tag{8}$$

where $L(r_s)$ is a coefficient that depends on the uncertainty about the location of the eavesdropper, and is given by (9), as shown at the bottom of the next page. Moreover, ${}_2F_1(\cdot,\cdot,\cdot,\cdot)$ is the Gaussian hypergeometric function [16, Eq. (9.111)].

Proof: Please refer to Appendix B. ∎

A. An Insightful Scenario

Next, we study the insightful scenario, when $\alpha = 2$. This path loss parameter corresponds to the free-space transmission, which even though is not a realistic case for terrestrial wireless communications, it provides useful insights for the impact of the uncertainty in Eve's location on the secrecy capacity. By substituting $\alpha = 2$ into (9), and applying [16, Eq. (9.121/6)], $L(r_s)$ can be simplified as

$$L^{\text{fs}}(r_s) = \frac{2^{r_s}\left(1+d_B^2\right)}{R_2^2 - R_1^2}\exp\left[-\frac{\left(1+d_B^2\right)(2^{r_s}-1)N_0}{E_s}\right] \times \ln\left(\frac{1+2^{r_s}\left(1+d_B^2\right)+R_2^2}{1+2^{r_s}\left(1+d_B^2\right)+R_1^2}\right). \tag{10}$$

Next, we examine the case where R_1 approaches R_2. Consider the function $l^{\text{fs}}(R_1) = L^{\text{fs}}(r_s)$ for a fixed r_s. We observe that $l^{\text{fs}}(R_1)$ is a decreasing function. In other words, as R_1 decreases, i.e., Alice becomes more uncertain about the location of the eavesdropper, the SOP also increases. By applying L' Hospital's rule on (10), we obtain

$$\lim_{R_1 \to R_2} l^{\text{fs}}(R_1) = \frac{2^{r_s}\left(1+d_B^2\right)\exp\left[-\frac{\left(1+d_B^2\right)(2^{r_s}-1)N_0}{E_s}\right]}{1+2^{r_s}\left(1+d_B^2\right)+R_2^2}. \tag{11}$$

By substituting (11) into (8), the SOP when $R_1 \to R_2$ can be written as

$$P_o^{\text{fs}}(r_s) = 1 - \frac{\exp\left[-\frac{\left(1+d_B^2\right)(2^{r_s}-1)N_0}{E_s}\right]}{1+2^{r_s}\frac{1+d_B^2}{1+R_2^2}}. \tag{12}$$

Note that (12) coincides with the SOP for a fixed eavesdropper distance from Alice, considering free-space transmission [17]. This indicates that as the uncertainty on the location of the eavesdropper decreases, the performance of the system tends to the system, where the location of the eavesdropper is considered to be known to Alice. This observation is illustrated in Section IV through simulations.

IV. Numerical Results and Discussion

We consider that Bob is located 3 m from Alice. Additionally, Alice knows that Eve is located in a ring with inner radius R_1 and outer radius R_2. Unless otherwise stated, $R_2 = 200$ m. In the following figures, LU stands for location uncertainty.

Fig. 1 depicts the SOP as a function of $\frac{E_s}{N_0}$ for different values of r_s, when $R_1 = 50$ m and $\alpha = 3$. Moreover, the SOP is plotted for the case when Eve's location is known ($d_E = R_1$ and $d_E = R_2$), in order to be used as benchmark. As expected, for a fixed targeted secrecy rate, $r_s \neq 0$, as $\frac{E_s}{N_0}$ increases, the SOP decreases. However, for $r_s = 0$, it is independent of the $\frac{E_s}{N_0}$. Furthermore, for a given $\frac{E_s}{N_0}$, as r_s increases

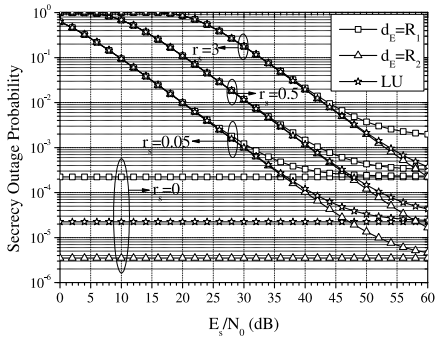

Fig. 1. The SOP as a function of E_s/N_0 for different values of r_s.

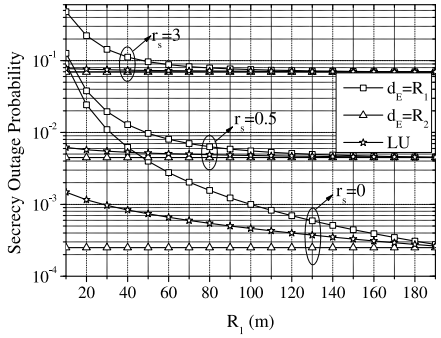

Fig. 2. The SOP as a function of R_1 for different values of R_s.

the SOP increases. We also observe that, when the distance between Alice and Eve is known and equal to $d_E = R_1$, the SOP is higher compared to the case where Eve's location is uncertain. However, when $d_E = R_2$, the SOP is lower, compared to the case with location uncertainty for Eve. In other words, the cases where Eve is located at a fixed distance equal to R_1 or R_2 from Alice can be treated as an upper or a lower bound, respectively, for the SOP. These observations reveal the importance of taking into consideration the uncertainty on the location of the eavesdropper, when designing and deploying a wireless system with PHY security.

Fig. 2 depicts the SOP as a function of R_1, for different values of r_s, when $\frac{E_s}{N_0} = 30$ dB and $\alpha = 2$. Again, the SOPs when the eavesdropper locations are known ($d_E = R_1$ and $d_E = R_2$) are illustrated as benchmarks. As expected, for a given r_s, as R_1 increases, the uncertainty of the Eve's received SNR decreases; hence, the SOP decreases. Also, we observe that for a fixed R_1, higher values of r_s lead to higher SOPs. As mentioned before, the cases where the distance is fixed and equal to $d_E = R_1$ and $d_E = R_2$ provide an upper and a lower

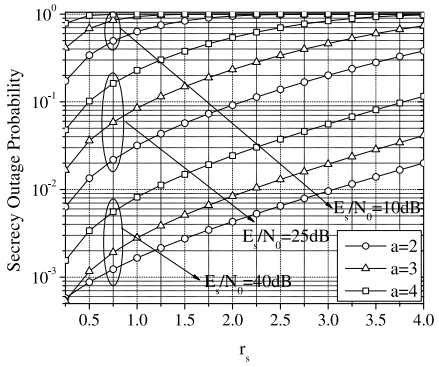

Fig. 3. The SOP as a function of R_s for different values of α.

bound, respectively, for the SOP. As $R_2 - R_1$ decreases, the uncertainty of Eve's location decreases, and the upper and the lower bound of the SOP converge.

Fig. 3 depicts the SOP as a function of r_s, for different values of α and $\frac{E_s}{N_0}$. We observe that, for fixed α and $\frac{E_s}{N_0}$, as r_s increases, the SOP increases. This is expected since, as indicated by (7), the instantaneous capacity difference between C_B and C_E is statistically less likely to achieve for higher values of r_s. Also, for a fixed $\frac{E_s}{N_0}$ and r_s, as α increases, the impact of path loss becomes more severe; therefore, the SOP increases. Moreover, for a fixed α and r_s, higher values of $\frac{E_s}{N_0}$ lead to lower values of the SOP. Additionally, it is evident that, in the low $\frac{E_s}{N_0}$ regime, it is not possible to achieve PHY security, since the SOP is very high. For example, for $\frac{E_s}{N_0} = 10$ dB and $\alpha = 4$, the SOP is always very close to 1, which means that PHY security is not feasible in this case. These results reveal the importance of taking both the effects of path loss and eavesdropper's location uncertainty into consideration, in the design and deployment of a wireless system with PHY security.

APPENDIX A
PROOF OF PROPOSITION 1

Since Eve's location is uniformly distributed as described in Section II, the CDF of $|h_E|^2$ can be evaluated as [13, Eq. (3)]

$$F_{|h_E|^2}(x) = \frac{2}{R_2^2 - R_1^2} \int_{R_1}^{R_2} z F_{|g_E|^2}\big(x\big(z^\alpha + 1\big)\big) dz, \qquad (13)$$

where $F_{|g_E|^2}(x)$ denotes the CDF of $|g_E|^2$, which, since $|g_E|^2$ is an exponentially distributed RV, is given by

$$F_{|g_E|^2}(x) = 1 - \exp(-x). \qquad (14)$$

$$f_{|h_E|^2}(x) = \frac{2\Big(E_{\frac{a-2}{\alpha}}\big(R_1^a x\big) + R_1^\alpha E_{-\frac{2}{\alpha}}\big(R_1^\alpha x\big)\Big)R_1^2 - 2\Big(E_{\frac{\alpha-2}{\alpha}}\big(R_2^\alpha x\big) + R_2^\alpha E_{-\frac{2}{\alpha}}\big(R_2^\alpha x\big)\Big)R_2^2}{\big(R_2^2 - R_1^2\big)\alpha} \exp(-x) \qquad (5)$$

$$L(r_s) = \frac{2^{r_s}\big(1 + d_B^\alpha\big)}{\big(1 + 2^{r_s} + d_B^\alpha 2^{r_s}\big)\big(R_2^2 - R_1^2\big)} \exp\left[-\frac{N_0\big(1 + d_B^\alpha\big)(2^{r_s} - 1)}{E_s}\right] \times \left({}_2F_1\left(1, \frac{2}{\alpha}, \frac{2+\alpha}{\alpha}, -\frac{R_2^\alpha}{1 + 2^{r_s} + d_B^\alpha 2^{r_s}}\right)R_2^2 - {}_2F_1\left(1, \frac{2}{\alpha}, \frac{2+\alpha}{\alpha}, -\frac{R_1^\alpha}{1 + 2^{r_s} + d_B^\alpha 2^{r_s}}\right)R_1^2\right) \qquad (9)$$

By substituting (14) into (13), we get

$$F_{|h_E|^2}(x) = 1 - \frac{2\exp(-x)}{R_2^2 - R_1^2} \int_{R_1}^{R_2} z \exp\left(-xz^{\alpha}\right) dz. \quad (15)$$

By setting $y = z^2$ into the integral in (15) and then by applying [16, Eq. 2.33/4], we get (6).

The PDF of $|h_E|^2$ can be obtained as

$$f_{|h_E|^2}(x) = \frac{\mathrm{d}F_{|h_E|^2}(x)}{\mathrm{d}x}. \quad (16)$$

By using (16) in (6), we get (5). This concludes the proof.

APPENDIX B
PROOF OF THEOREM 1

The SOP can be expressed as

$$P_o(r_s) = P_r\left(\frac{X}{Y} \leq 2^{r_s}\right), \quad (17)$$

where $X = \gamma_B + 1$ and $Y = \gamma_E + 1$.

Since $|h_B|$ is a Rayleigh distributed RV, it follows that $|h_X|^2$ is an exponentially distributed RV. Taking into consideration (2), the CDF of the SNR at Bob is given by

$$F_{\gamma_B}(x) = 1 - \exp\left(-\frac{\left(1 + d_B^{\alpha}\right)N_0}{E_s}x\right). \quad (18)$$

Consequently, the CDF of X can be derived as $F_X(x) = F_{\gamma_B}(x-1)$, or

$$F_X(x) = 1 - \exp\left(-\frac{\left(1 + d_B^{\alpha}\right)(x-1)N_0}{E_s}\right). \quad (19)$$

On the other hand, the SNR of the eavesdropper is a RV that follows a distribution described in Proposition 1. Therefore, by using (15) and (16), the PDF of Y can be expressed as

$$f_Y(y) = \frac{2N_0}{(R_2^2 - R_1^2)E_s} \int_{R_1}^{R_2} z\left(1 + z^{\alpha}\right) \times \exp\left(-\frac{(1 + z^{\alpha})(x-1)N_0}{E_s}\right) dz. \quad (20)$$

Furthermore, since X and Y are independent RVs, by taking into consideration (17), the SOP can be obtained as

$$P_o(r_s) = \int_1^{\infty} F_X\left(2^{r_s}x\right) f_Y(x) dx. \quad (21)$$

By substituting (19) and (20) into (21), and after some simplifications, we obtain

$$P_o(r_s) = 1 - \frac{2N_0}{(R_2^2 - R_1^2)E_s} \int_{R_1}^{R_2} z(1 + z^{\alpha}) \exp\left(\frac{N_0}{E_s}\left(z^{\alpha} - d_B^{\alpha}\right)\right) \times \int_1^{\infty} \exp\left(-\frac{N_0}{E_s}\left(2^{r_s} + 2^{r_s}d_B^{\alpha} - 1 - z^{\alpha}\right)x\right) dx dz. \quad (22)$$

After evaluating the internal integral, (22) becomes

$$P_o(r_s) = 1 - \frac{2}{R_2^2 - R_1^2} \exp\left(-\frac{\left(1 + d_B^{\alpha}\right)(2^{r_s} - 1)N_0}{E_s}\right) \times \int_{R_1}^{R_2} \frac{z(1 + z^{\alpha})}{1 + 2^{r_s} + d_B^{\alpha}2^{r_s} + z^{\alpha}} dz. \quad (23)$$

Finally, we carry out the integration in (23) by using [16, Eq. (9.111)], and after some mathematical manipulations, we get (8). This concludes the proof.

REFERENCES

[1] D.-B. Ha, T. Q. Duong, D.-D. Tran, H. J. Zepernick, and T. T. Vu, "Physical layer secrecy performance over Rayleigh/Rician fading channels," in *Proc. Int. Conf. Adv. Technol. Commun.*, Hanoi, Vietnam, Oct. 2014, pp. 113–118.

[2] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[3] L. J. Rodriguez *et al.*, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[4] A.-A. A. Boulogeorgos, D. S. Karas, and G. K. Karagiannidis, "How much does I/Q imbalance affect secrecy capacity?" *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1305–1308, Jul. 2016.

[5] M. Ghogho and A. Swami, "Characterizing physical-layer secrecy with unknown eavesdropper locations and channels," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Prague, Czech Republic, May 2011, pp. 3432–3435.

[6] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, South Korea, Jun. 2009, pp. 2442–2446.

[7] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.

[8] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in Rician wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2780–2791, Apr. 2016.

[9] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.

[10] C. Liu and R. A. Malaney. (May 2016). *Location-Based Beamforming and Physical Layer Security in Rician Wiretap Channels*. [Online]. Available: http://arxiv.org/abs/1604.06143

[11] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2627–2631.

[12] H. Wang, X. Zhou, and M. C. Reed, "On the physical layer security in large scale cellular networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Shanghai, China, Apr. 2013, pp. 2462–2467.

[13] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Process. Lett.*, vol. 21, no. 12, pp. 1501–1505, Dec. 2014.

[14] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[15] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover, 1974.

[16] I. S. Gradshteĭn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. New York, NY, USA: Academic Press, 2000.

[17] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.