Backing off from Rayleigh and Rice: Achieving Perfect Secrecy in Wireless Fading Channels

Pablo Ramírez-Espinosa[(1)], F. Javier López-Martínez[(2)].
pres@es.aau.dk, fjlopezm@ic.uma.es
[(1)]Connectivity Section, Dept. Electronic Systems, Aalborg University, Aalborg Øst 9220, Denmark.
[(2)]Dpto. Ingeniería de Comunicaciones, Universidad de Málaga, Malaga 29071, Spain

***Abstract*—We show that for a legitimate communication under multipath quasi-static fading with a reduced number of scatterers, it is possible to achieve perfect secrecy even in the presence of a passive eavesdropper for which no channel state information is available. Specifically, we show that the outage probability of secrecy capacity (OPSC) is zero for a given range of average signal-to-noise ratios (SNRs) at the legitimate and eavesdropper's receivers. As an application example, we analyze the OPSC for the case of two scatterers, explicitly deriving the relationship between the average SNRs, the secrecy rate R_S and the fading model parameters required for achieving perfect secrecy.**

I. INTRODUCTION

The seminal works in [1–3] have boosted the interest for providing secure communications over wireless channels from an information-theoretic viewpoint based on the classical work by Shannon [4]. Compared to the case in which fading is neglected [5, 6], the effect of random fluctuations due to fading turns out being beneficial in some instances [2, 3]. However, when channel state information (CSI) of the eavesdropper is unknown at the legitimate transmitter, these previous works [1–3] show that it is not possible to ensure *perfect secrecy* in wireless fading channels, and only a probabilistic measure is available through the outage probability of secrecy capacity (OPSC) [1].

Wireless physical layer security (PLS) has now become a rather mature field and numerous works characterize the key performance metrics under different propagation conditions, but always relying on the central limit theorem (CLT) assumption that gives rise to the Rician and Rayleigh models, or generalizations of these [7–9]. Nowadays, because of the new use cases of wireless systems under the umbrella of 5G and its evolutions, there are several examples in which the propagation conditions may be substantially different to those predicted by state-of-the-art fading models. For instance, in mmWave communications, a scarce number of multipath components arrives at the receiver [10], so that diffuse scattering only becomes relevant when non-line-of-sight (NLoS) conditions are considered [11]. In a different context, the potential of reconfigurable intelligent surfaces (RIS) [12, 13] to design the amplitude and phases of the scattered waves in order to optimize system performance can also be translated into a superposition of a finite number of individual waves.

Due to the great deal of attention received by these aforementioned emerging scenarios, we revisit in this work the issue of secure communications over wireless channels, with one key question in mind: *What's the effect of considering a finite number of scatterers on wireless physical layer security?* Thanks to the fine-grain characterization of the wireless propagation captured by ray-based models, we demonstrate for the first time that it is possible to achieve *perfect secrecy* in the communication between two legitimate peers under multipath quasi-static fading, i.e., *zero* OPSC, when a reduced number of scatterers is considered. We determine the conditions under which perfect secrecy can be ensured, and then we give some practical examples using a ray-based fading model.

This work is funded by the Spanish Government and the European Fund for Regional Development FEDER (project TEC2017-87913-R) and by Junta de Andalucia (project P18-RT-3175, TETRA5G). The authors acknowledge the assistance of R. José Sánchez-Alarcón on early stages of this work.

II. PROBLEM FORMULATION

A. System model for PLS

We consider a legitimate user (Alice) who wants to send confidential messages to another user (Bob) in the presence of an eavesdropper (Eve). For simplicity, yet without loss of generality, all these agents are equipped with single-antenna devices. The complex channel gains from Alice to Bob and Eve are denoted by h_b and h_e, respectively, and assumed constant during the transmission of an entire codeword but independent from one codeword to the next one, i.e., we consider quasi-static fading channels. Hence, the instantaneous signal-to-noise ratios (SNRs) at Bob and Eve are given by

$$\gamma_b = \overline{\gamma}_b \frac{\|h_b\|^2}{\mathbb{E}[\|h_b\|^2]}, \qquad \gamma_e = \overline{\gamma}_e \frac{\|h_e\|^2}{\mathbb{E}[\|h_e\|^2]}, \tag{1}$$

where $\mathbb{E}[\cdot]$ is the expectation operator and $\overline{\gamma}_b$ and $\overline{\gamma}_e$ denote the average SNR at Bob and Eve, respectively.

If Alice has perfect knowledge of both Bob's and Eve's instantaneous CSI, perfect secrecy can be obtained by adapting the transmision rate, R_s, in those instants where $\gamma_b > \gamma_e$ [1, 3]. The secrecy capacity, i.e., the maximum rate ensuring a secure communication between Alice and Bob, is [5, 6]:

$$C_s = [C_b - C_e]^+ = [\log_2(1+\gamma_b) - \log_2(1+\gamma_e)]^+, \tag{2}$$

where C_b and C_e are the capacities of Bob and Eve, respectively, and $[x]^+$ is the shorthand notation for $\max\{0, x\}$. Thus, for each channel realization, Alice would transmit at a rate $R_s \leq C_s$ in order to avoid any information leakage to Eve.

Consider now the case of a purely passive eavesdropper, for which Eve's CSI is unknown at the transmitter. In this situation, previous works state that perfect secrecy cannot be achieved, and therefore they resort on outage analysis [1–3]. That is, Alice would blindly transmit at a target rate R_s under the assumption that $C_s \geq R_s$. If $C_s < R_s$, then an outage occurs and the security of the transmission is compromised with some probability, i.e., the OPSC defined [1] as

$$P_{\text{out}}(R_s) \triangleq P\{C_s < R_s\}. \tag{3}$$

B. *CLT and ray-based fading models*

Due to the multipath propagation, the complex based-band received signals are written as the superposition of multiple waves arising from reflections and scattering as [7, eq. (1)]

$$h_k = \sum_{i=1}^{N_k} V_{i,k} e^{j\phi_{i,k}}, \tag{4}$$

where $k = b, e$ denotes indistinctly Bob's or Eve's channel, N_k denotes the number of multipath waves, $V_{i,k} \in \mathbb{R}^+$ their constant amplitudes and $\phi_{i,k}$ their phases, assumed to be independent and uniformly distributed over $[0, 2\pi)$. The sum in (4) can be split into two groups of waves as

$$h_k = \sum_{i=1}^{M_k} V_{i,k} e^{j\phi_{i,k}} + \sum_{i=1}^{P_k} \widehat{V}_{i,k} e^{j\theta_{i,k}} \tag{5}$$

where $\theta_{i,k}\ \forall\ i$ are also independent and uniformly distributed. Hence, the first sum represents the contribution of the M_k dominant or specular components, whilst the second one groups the contribution of non-specular or diffuse waves, where the power of each component is considerably lower. When P_k is sufficiently large, i.e., we have a rich multipath propagation, the diffuse component can be regarded as Gaussian because of the CLT, and therefore

$$h_k|_{P_k \to \infty} = \sum_{i=1}^{M_k} V_{i,k} e^{j\phi_{i,k}} + \sigma_{x,k} X_k + j\sigma_{y,k} Y_k \tag{6}$$

with $X_k, Y_k \sim \mathcal{N}(0,1)$ and $\sigma_{x,k}, \sigma_{y,k} \in \mathbb{R}^+$.

Equation (6) is the basis for most popular fading models, which typically arise depending on the value of the parameters M_k, $\sigma_{x,k}$ and $\sigma_{y,k}$. For instance, if $\sigma_{x,k} = \sigma_{y,k}$ and $M_k = 0$ we obtain the Rayleigh model, whilst $M_k = 1$ yields the Rice distribution and $M_k = 2$ reduces to the two-wave with diffuse power (TWDP) model [7]. While previous works consider channel gains according to (6), we will stick to the general formulation in (4) in order to explicitly account for the effect of considering a *finite* number of multipath waves on PLS.

III. Perfect Secrecy over Fading Channels

A. *Impact of a reduced number of scatterers in OPSC*

In order to better understand the influence of the fading distribution in the OPSC, we reformulate P_{out} in (3) in terms of Bob's and Eve's SNRs as

$$P_{\text{out}}(R_s) = P\{\gamma_b < 2^{R_s}\gamma_e + 2^{R_s} - 1\} = P\{\gamma_b < \gamma_{\text{eq}}\}, \tag{7}$$

which is obtained by introducing (2) in (3) and performing some basic algebraic manipulations. Note that, when conditioning on γ_e, P_{out} corresponds to the cumulative distribution function (CDF) of γ_b and, therefore, it can be computed by averaging over all the possible states of γ_e as

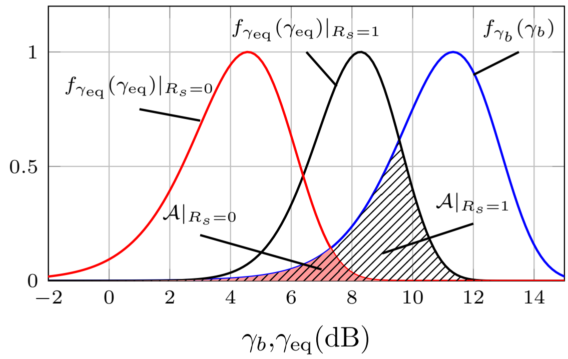
$$P_{\text{out}}(R_s) = \int_0^\infty F_{\gamma_b}\left(2^{R_s}\gamma_e + 2^{R_s} - 1\right) f_{\gamma_e}(\gamma_e)\, d\gamma_e. \tag{8}$$

Regarding (7), it is clear that the condition for secrecy is $\gamma_b > \gamma_{\text{eq}}$, where $\gamma_{\text{eq}} = 2^{R_s}\gamma_e + 2^{R_s} - 1$. From a geometric point of view, for a given value of γ_{eq}, the OPSC corresponds therefore to the area under the probability density function (PDF) of γ_b for which $\gamma_b < \gamma_{\text{eq}}$. If we consider the complete distribution of γ_{eq}, then the outage probability is related to the common area under the PDFs of γ_b and γ_{eq}, being the latter a rescaled and shifted version of $f_{\gamma_e}(\gamma_e)$ of the form

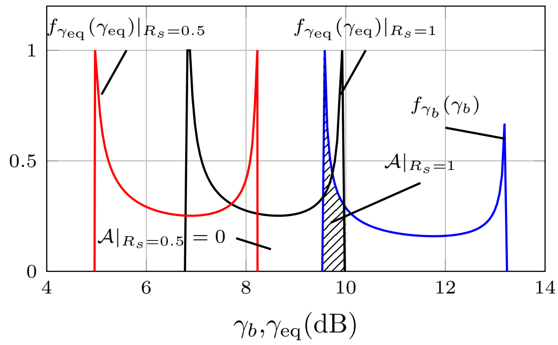
$$f_{\gamma_{\text{eq}}}(\gamma_{\text{eq}}) = 2^{-R_s} f_{\gamma_e}(2^{-R_s}(\gamma_{\text{eq}} + 1) - 1). \tag{9}$$

Thus, the larger this overlapped area in which γ_b can take lower values than γ_{eq}, the higher the outage probability. If we consider any fading distribution arising from the CLT assumption, i.e., the underlying random variables are Gaussian distributed, the PDFs of the SNRs – or, equivalently, those of $\|h\|^2$ – are supported on a semi-infinite interval $[0, \infty)$, and then the tails of $f_{\gamma_b}(\gamma_b)$ and $f_{\gamma_{\text{eq}}}(\gamma_{\text{eq}})$ overlap regardless of the values of R_s and the average SNRs. Hence, the condition of $\gamma_b < \gamma_{\text{eq}}$ is met with non-null probability and perfect secrecy cannot be achieved [1–3]. This can be observed in Fig. 1a, where even for $R_s = 0$ there exists some outage area $\mathcal{A}$.

However, things are different when assuming ray-based fading models. Due to the consideration of a finite number of waves, there is a maximum and a minimum value for both the channel gains and the instantaneous SNRs, i.e., the PDFs of γ_b and γ_{eq} are supported on a bounded interval, say $[\gamma^{\min}, \gamma^{\max}]$. These limit values will depend on the relative amplitudes of the incident waves, that will add-up destructively/constructively with some probability. Therefore, it is evident that in some cases the distribution domains will be disjoint, and hence the OPSC can be identically zero, as showed in Fig. 1b. That is, under certain conditions, any possible value of γ_b will always be larger than γ_{eq}. This is an important observation, since it will allow us to achieve perfect secrecy for transmission rates $R_s > 0$ without Eve's CSI knowledge at the transmitter.



(a) γ_b and γ_{eq} follow a CLT fading distribution (Rician).



(b) γ_b and γ_{eq} follow a ray-based fading distribution.

Fig. 1: Common area under the PDFs of γ_b and γ_{eq} for classical and ray-based fading models, and different values of R_s ($\overline{\gamma_b} = 12$ dB and $\overline{\gamma_e} = 5$ dB). For better visualization, the PDFs in the figure have been normalized.

B. Achieving perfect secrecy over ray-based fading channels

Let us consider that the gains for both Eve's and Bob's channels are given by (4). For simplicity — yet without loss of generality — we assume that $V_{1,k} \geq V_{2,k} \geq \cdots \geq V_{N_k,k}$. It is clear that the maximum value of h_k, where $k = b, e$ is used again to distinguish between Bob's and Eve's gains, is obtained when all the waves in (4) are summed coherently. In turn, the minimum value arises when destructive combination occurs. Consequently, and in stark contrast with classical fading distributions, the domain of $\|h_k\|$ is bounded on the interval $[\|h_k^{\text{min}}\|, \|h_k^{\text{max}}\|]$ with

$$\|h_k^{\text{min}}\| = \left[V_{1,k} - \sum_{i=2}^{N_k} V_{i,k}\right]^+, \quad \|h_k^{\text{max}}\| = \sum_{i=1}^{N_k} V_{i,k}. \quad (10)$$

Therefore, this finite domain definition of channel gains allows us to achieve zero OPSC when a certain condition is met, as stated in the following proposition.

Proposition 1. *Consider h_b and h_e as in (4). Then, for a given transmission rate $R_s > 0$, perfect secrecy, i.e., $P_{out}(R_s) = 0$, is achieved if*

$$\gamma_b^{min} > 2^{R_s}\gamma_e^{max} + 2^{R_s} - 1, \quad (11)$$

where γ_b^{min} and γ_e^{max} are given by

$$\gamma_b^{min} = \overline{\gamma}_b \frac{\|h_b^{min}\|^2}{\mathbb{E}[\|h_b\|^2]}, \qquad \gamma_e^{max} = \overline{\gamma}_e \frac{\|h_e^{max}\|^2}{\mathbb{E}[\|h_e\|^2]} \quad (12)$$

with $\|h_b^{min}\|$ and $\|h_e^{max}\|$ as in (10) and

$$\mathbb{E}[\|h_k\|^2] = \sum_{i=1}^{N_k} V_{i,k}^2, \quad k = b, e. \quad (13)$$

Proof: The condition for zero OPSC is given by $\gamma_b^{\text{min}} > \gamma_{\text{eq}}^{\text{max}}$. Since γ_{eq} is obtained as a linear transformation over γ_e, its maximum value occurs when $\gamma_e = \gamma_e^{\text{max}}$, yielding immediately (11). On the other hand, (13) is obtained by calculating the expectation of the squared modulus of (4) and applying the multinomial theorem. ∎

Inspecting (11), we observe that higher values of R_s imply a more restrictive perfect secrecy condition, i.e., if we aim to increase the transmission rate, we need γ_b^{min} to be larger. This is also shown in Fig. 1, where increasing R_s shifts $f_{\gamma_{\text{eq}}}$ to the right regardless of the considered fading distribution. Moreover, as $\overline{\gamma}_b$ becomes larger – or, equivalently, $\overline{\gamma}_e$ takes lower values – we can transmit at a faster secure rate while keeping zero OPSC, which is a coherent result.

We also observe that considering a larger number of rays in (4) has a significant impact in the OPSC. As N_k increases, either in Bob's or Eve's channel, the interval $[h_k^{\text{min}}, h_k^{\text{max}}]$ gets wider, causing the condition in (11) to be more restrictive. In fact, if $N \to \infty$, then (4) becomes a Gaussian random variable, rendering the classical fading distributions and implying that $\|h_k^{\text{min}}\| \to 0$ and $\|h_k^{\text{max}}\| \to \infty$, as predicted by CLT-based channel modeling approaches.

It is important to note that although Eve's instantaneous CSI is not required, we implicitly make some assumptions regarding the distribution of h_e, i.e., the value of γ_e^{max}, in order to apply the secrecy condition in (11). Because the relative amplitudes of the waves arriving at Eve as well as their average power are closely related to the geometry of the scenario under analysis, this is equivalent to assume that Alice has information over the propagation environment.

More specifically, some worst-case assumptions (equivalent to having statistical knowledge of CSI without explicitly requiring it) can be taken and still ensure perfect secrecy. For instance, an upper bound for the average SNR at Eve ($\overline{\gamma}_e$) can be determined by establishing exclusion areas (or secure areas) around the transmitter in which no eavesdroppers can be placed [14]. With the radius of the secure area, it is possible to calculate the minimum pathloss to Eve and therefore we can upper bound its average SNR. Similarly, the number of rays arriving at the eavesdropper can be designed from the geometry of the propagation scenario in case of highly directional transmissions, or by properly controlling the propagation environment using large/reconfigurable intelligent surfaces, which allow to modify at will the phases of the incident waves [12, 13]. Thus, although no CSI may be available for a purely passive eavesdropper, we can still design the transmission in order to ensure perfect secrecy.

IV. Secure TX over two-wave fading

After formulating the conditions on which perfect secrecy can be attained when considering ray-based fading channels, we now analyze a simple, albeit illustrative, case by assuming two dominant components arriving at both receiver ends. The two-wave (or two ray) fading model [7, 15] arises when setting $N_k = 2$ in (4), i.e.

$$h_k = V_{1,k}e^{j\phi_{1,k}} + V_{2,k}e^{j\phi_{2,k}}. \quad (14)$$

This model is completely characterized by the parameter $\Delta_k = \frac{2V_{1,k}V_{2,k}}{V_{1,k}^2+V_{2,k}^2}$, which measures the relative difference in amplitude between the two waves. Hence, $\Delta_k = 1$ implies that both rays have exactly the same power, whilst $\Delta_k = 0$ signifies that one of the specular components in (14) vanishes.

With this consideration, the PDF and the CDF of the SNR at Bob and Eve, defined in the interval $\gamma_k^{\text{min}} \leq \gamma_k \leq \gamma_k^{\text{max}}$, are written as [7, 16]

$$f_{\gamma_k}^{\text{tw}}(\gamma_k) = \frac{1}{\pi\overline{\gamma}_k\sqrt{\Delta_k^2 - (1-\gamma_k/\overline{\gamma}_k)^2}} \quad (15)$$

$$F_{\gamma_k}^{\text{tw}}(\gamma_k) = \frac{1}{2} - \frac{1}{\pi}\text{asin}\left(\frac{1-\gamma_k/\overline{\gamma}_k}{\Delta_k}\right) \quad (16)$$

where, as in the previous section, the subindex $k = b, e$ is used to distinguish between the parameters of Bob's and Eve's channel distributions. The domain boundaries for each distribution are calculated as in (12), yielding in this case

$$\gamma_k^{\text{min}} = \overline{\gamma}_k(1 - \Delta_k), \qquad \gamma_k^{\text{max}} = \overline{\gamma}_k(1 + \Delta_k), \quad (17)$$

and therefore the condition for perfect secrecy stated in Proposition 1 is expressed as

$$\overline{\gamma}_b > \frac{2^{R_s}\overline{\gamma}_e(1+\Delta_e)+2^{R_s}-1}{1-\Delta_b}. \quad (18)$$

Thus, despite the fact that Eve's instantaneous CSI is unkown at Alice, secrecy in the communication can be ensured if the average SNR at Bob is above a certain threshold. In case Alice does not have any statistical knowledge of Eve's channel, the transmission rate can be adapted based on the worst-case in which $\Delta_e = 1$. As previously indicated, when the average SNR at Eve is unknown, it can be upper-bounded

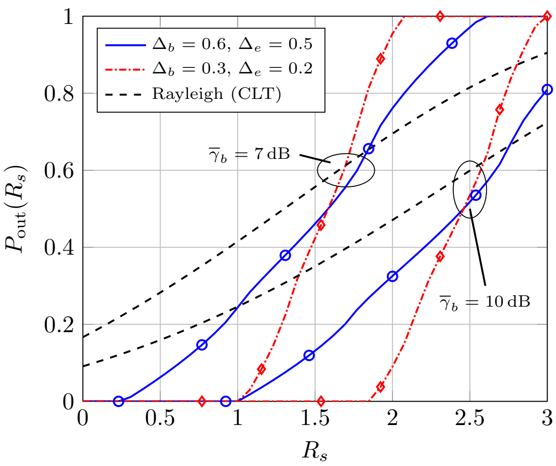


Fig. 2: Impact of CLT based fading models (Rayleigh) and ray-based ones (Two-wave) in the OPSC for different values of channel parameters and average SNRs. For all traces, $\overline{\gamma}_e = 0\,$dB. Solid lines correspond to theoretical calculations whilst markers correspond to Monte Carlo (MC) simulations.

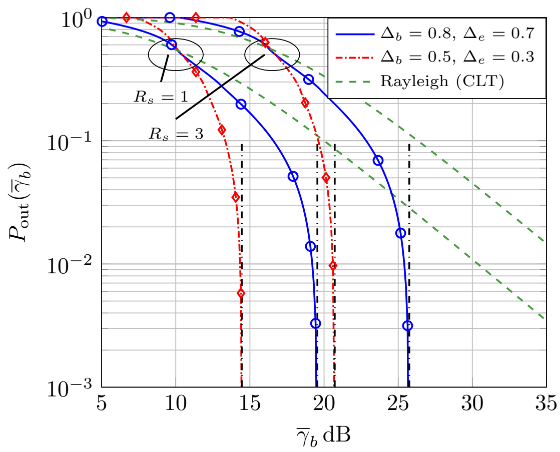


Fig. 3: OPSC in terms of $\overline{\gamma}_b$ for different values of channel parameters and distinct fading models. For all traces $\overline{\gamma}_e = 7\,$dB. Solid lines correspond to theoretical calculations whilst markers correspond to MC simulations. Dashdotted vertical lines correspond to the asymptotic OPSC.

by defining exclusion areas in which no eavesdroppers are possible. Hence, even in this situation, the perfect secrecy condition can be met, e.g., by a proper design of the distance between the transmitter and the legitimate receiver. After simple manipulations to (18), the largest constant rate that ensures perfect secrecy is expressed as

$$R_s^{\max} = \left[\log_2\left(\tfrac{\overline{\gamma}_b(1-\Delta_b)+1}{\overline{\gamma}_e(1+\Delta_e)+1}\right)\right]^+. \tag{19}$$

In fact, whenever Alice has perfect knowledge of Bob's CSI (instead of statistical knowledge only), it is possible to adapt its transmission rate to Bob's instantaneous CSI while meeting the condition $\gamma_b > \overline{\gamma}_e(1+\Delta_e)$, which yields the following expression for the instantaneous secrecy capacity:

$$C_s = \left[\log_2\left(\tfrac{\gamma_b+1}{\overline{\gamma}_e(1+\Delta_e)+1}\right)\right]^+ \geq R_s^{\max}. \tag{20}$$

The OPSC over two-wave fading is straightforwardly calculated by introducing (15) and (16) in (8), leading to

$$P_{\text{out}}^{\text{tw}}(R_s) = \frac{1}{\pi\overline{\gamma}_e}\int_{\gamma_e^{\min}}^{\gamma_e^{\max}} \frac{\widehat{F}_{\gamma_b}^{\text{tw}}\left(2^{R_s}\gamma_e + 2^{R_s} - 1\right)}{\sqrt{\Delta_e^2 - (1-\gamma_e/\overline{\gamma}_e)^2}}\, d\gamma_e. \tag{21}$$

The OPSC in (21) in terms of R_s and $\overline{\gamma}_b$ is depicted in Figs. 2 and 3, respectively. For the sake of comparison, P_{out} over CLT based channels (in this case, Rayleigh fading) is also shown as a reference. We observe that, for a given $R_s < R_s^{\max}$, the outage probability is exactly zero when considering a finite number of reflections, whilst this behavior is not reproduced when assuming a fading model arising from the CLT. Specifically, we observe that the asymptotic decay for the Rayleigh case (i.e., the negative slope of the OPSC as $\overline{\gamma}_b$ grows) is that of a diversity order equal to one. Conversely, when considering the ray-based alternatives here analyzed the OPSC abrutly drops for the limit value of $\overline{\gamma}_b$ given by (18), which can be regarded as an *infinite* diversity order.

V. Conclusions

We provided a new look at wireless PLS, backing off from the classical CLT assumption associated to fading and explicitly accounting for the effect of considering a finite number of multipath waves arriving the receiver ends. We established for the first time the conditions under which it is possible to achieve *perfect secrecy* in wireless channels even when the eavesdropper's CSI is unknown at the transmitter.

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, Jun. 2008.

[2] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470–2492, Jun. 2008.

[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[6] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[7] G. D. Durgin, T. S. Rappaport, and D. A. de Wolf, "New analytical models and probability density functions for fading in wireless communications," *IEEE Trans. Commun.*, vol. 50, pp. 1005–1015, Jun. 2002.

[8] M. Yacoub, "The κ-μ distribution and the η-μ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, pp. 68–81, Feb. 2007.

[9] J. M. Romero-Jerez, F. J. Lopez-Martinez, J. F. Paris, and A. J. Goldsmith, "The fluctuating two-ray fading model: statistical characterization and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 4420–4432, Jul. 2017.

[10] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges," *Wirel. Netw.*, vol. 21, pp. 2657–2676, Nov. 2015.

[11] D. Solomitckii, Q. C. Li, T. Balercia, C. R. C. M. da Silva, S. Talwar, S. Andreev, and Y. Koucheryavy, "Characterizing the impact of diffuse scattering in urban millimeter-wave deployments," *IEEE Wireless Commun. Lett.*, vol. 5, pp. 432–435, Aug. 2016.

[12] K. Ntontin, M. Di Renzo, J. Song, F. Lazarakis, J. de Rosny, D.-T. Phan-Huy, O. Simeone, R. Zhang, M. Debbah, G. Lerosey, *et al.*, "Reconfigurable intelligent surfaces vs. relaying: Differences, similarities, and performance comparison," *arXiv preprint arXiv:1908.08747*, 2019.

[13] L. Subrt and P. Pechac, "Intelligent walls as autonomous parts of smart indoor environments," *IET Commun.*, vol. 6, pp. 1004–1010, May 2012.

[14] P. C. Pinto, J. Barros, and M. Z. Win, "Secure Communication in Stochastic Wireless Networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 125–138, 2012.

[15] J. Frolik, "On appropriate models for characterizing hyper-rayleigh fading," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 5202–5207, Dec. 2008.

[16] P. C. F. Eggers, M. Angjelichinoski, and P. Popovski, "Wireless channel modeling perspectives for ultra-reliable communications," *IEEE Trans. Wireless Commun.*, vol. 18, pp. 2229–2243, Apr. 2019.