On Secure Transmission Design: An Information Leakage Perspective

Yong Huang[†], Wei Wang[*†], Biao He[‡], Liang Sun[§], Tao Jiang[†]
[†]School of Electronic Information and Communications, Huazhong University of Science and Technology
[‡] Department of Electrical Engineering and Computer Science, University of California, Irvine
[§] School of Electronic and Information Engineering, Beihang University
Email: {yonghuang, weiwangw, taojiang}@hust.edu.cn, biao.he@uci.edu, eelsun@buaa.edu.cn

Abstract—**Information leakage rate is an intuitive metric that reflects the level of security in a wireless communication system, however, there are few studies taking it into consideration. Existing work on information leakage rate has two major limitations due to the complicated expression for the leakage rate: 1) the analytical and numerical results give few insights into the trade-off between system throughput and information leakage rate; 2) and the corresponding optimal designs of transmission rates are not analytically tractable. To overcome such limitations and obtain an in-depth understanding of information leakage rate in secure wireless communications, we propose an approximation for the average information leakage rate in the fixed-rate transmission scheme. Different from the complicated expression for information leakage rate in the literature, our proposed approximation has a low-complexity expression, and hence, it is easy for further analysis. Based on our approximation, the corresponding approximate optimal transmission rates are obtained for two transmission schemes with different design objectives. Through analytical and numerical results, we find that for the system maximizing throughput subject to information leakage rate constraint, the throughput is an upward convex non-decreasing function of the security constraint and much too loose security constraint does not contribute to higher throughput; while for the system minimizing information leakage rate subject to throughput constraint, the average information leakage rate is a lower convex increasing function of the throughput constraint.**

I. Introduction

The inherent openness of wireless channel makes data transmission difficult to shield from unintended recipients [1]. Although the security of wireless transmission is safeguarded by traditional cryptographic techniques, an eavesdropper with a strong computational ability still can decipher confidential information from the received symbols by using brute-force attacks [2]. In this situation, the transmitted information is completely leaked to the eavesdropper over wireless channel, which is the worst throughput-information leakage rate relation for securing wireless transmission. Physical layer security has been proposed in [3] for ensuring secure wireless communications by exploiting the characteristics of wireless channels without any assumption on the computation capability of the eavesdropper. With the help of physical layer security, more confidential information could be transmitted on secure wireless transmission by introducing random noises into the transmitted messages to confuse the eavesdropper. Hence, it is of great interest to investigate the throughput-information leakage rate trade-off on secure transmission system.

Although there are many secure transmission designs taking throughput into account, limited studies on information leakage rate are found in the literature. Specifically, [4] proposed the average information leakage rate over quasi-static fading channels, which tells how fast on average the information is leaked to the eavesdropper, and examines average information leakage rate in secure transmission design. The major limitations in [4] are: 1) the analytical and numerical results give few insights into the trade-off between system throughput and information leakage rate; 2) and the corresponding optimal designs of transmission rates are not analytically tractable. Besides, implicit exponential integral function is involved in the average information leakage rate, which hinders the further research on information leakage rate in wireless communication systems.

In this work, we study the secure transmission design from an information leakage perspective. To address the above limitations, we reasonably approximate average information leakage rate and, based on the approximation, two transmission systems are considered. The major contributions of this paper are:

- We thoroughly study the secure transmission design from an information leakage perspective. We propose a reasonable approximation for average information leakage rate. Based on the approximation, for the system maximizing throughput subject to information leakage rate constraint, we obtain the closed-form approximate optimal secure transmission rates; for the system minimizing information leakage rate subject to throughput constraint, we get the low-complexity approximate optimal secure transmission rates.
- Based on the derived approximations, the throughput-information leakage rate trade-offs over wireless communication systems are comprehensively investigated. It is found that for the system maximizing throughput subject to information leakage rate constraint, the throughput is an upward convex non-decreasing function of security constraint. However, for the system minimizing information leakage rate subject to throughput constraint, the

[*]The Corresponding author is Wei Wang (weiwangw@hust.edu.cn).

978-1-5386-4727-1/18/$31.00 ©2018 IEEE

average information leakage rate is a lower convex increasing function of the throughput constraint. In the both systems, too stringent or too loose throughput constraints will suffer the systems.

The remainder of this paper is organized as follows. In section II, we illustrate the secure transmission and problem formulation, and in section III we detail the system design with the proposed approximation. Next, section IV shows the numerical results. Finally, the paper is concluded in section V.

II. Secure Transmission and Problem Formulation

We consider the wiretap-channel system, where a transmitter, Alice, sends confidential information to an intended receiver, Bob, in the presence of an eavesdropper, Eve. Alice, Bob and Eve are assumed to all have a single antenna. We refer to the Alice-Bob channel as the main channel and the Alice-Eve channel as the eavesdropper's channel. Both channels are assumed to undergo independent quasi-static fading. Then, the instantaneous channel capacity of Bob or Eve is given by

$$C_i = \log_2 (1 + \gamma_i), i = b \text{ or } e, \tag{1}$$

where γ_i denotes the instantaneous signal-to-noise ratios (SNRs), the subscripts b and e denote Bob and Eve, respectively. We adopt the quasi-static Rayleigh fading channel model, and the instantaneous SNR has an exponential distribution, which is given by

$$f(\gamma_i) = \frac{1}{\bar{\gamma}_i} \exp\left(-\frac{\gamma_i}{\bar{\gamma}_i}\right), i = b \text{ or } e, \tag{2}$$

where $\bar{\gamma}_i$ denotes the average received SNR at Bob or Eve.

A. Secure Encoding

We consider the widely-adopted wiretap code [5] for confidential message transmissions. Specifically, there are two transmission rates, namely, the codeword transmission rate, R_b, and the confidential information rate, R_s. The rate cost for providing secrecy is defined as the positive rate difference between R_b and R_s, which is expressed as

$$\phi = R_b - R_s. \tag{3}$$

The rate cost indicates the extra bits to introduce randomness for providing secrecy against the eavesdropper [6] in a codeword. A length n wiretap code is constructed by generating 2^{nR_b} codewords $x^n(w, v)$, where $w = 1, 2, \cdots, 2^{nR_s}$ and $v = 1, 2, \cdots, 2^{n(R_b - R_s)}$. For each message index w, we randomly select v from $\left\{1, 2, \cdots, 2^{n(R_b - R_s)}\right\}$ with uniform probability and transmit the codeword $x^n(w, v)$.

B. Transmission Scheme

In this paper, we consider a fixed-rate transmission scheme, where the transmission rates, i.e., R_b and R_s, are fixed over time. Bob and Eve are assumed to perfectly know their own channels. Hence, the values of C_b and C_e are known by Bob and Eve, respectively. Alice has the statistical knowledge of Bob and Eve's channels but does not know about the instantaneous channel capability. We further assume that Bob provides a one-bit feedback about his channel quality to Alice in order to avoid unnecessary transmissions [7], [8]. The one-bit feedback enables an on-off transmission scheme to avoid connection outage. It is assumed that the transmission takes place only when $R_b \leq C_b$ [4]. Therefore, the on-off transmission scheme incurs a probability of transmission, which is given by

$$p_{tx} = \mathbb{P}(R_b \leq C_b) = \exp\left(-\frac{2^{R_b} - 1}{\bar{\gamma}_b}\right). \tag{4}$$

C. Metrics

We adopt the average information leakage rate and the throughput to measure the secrecy performance and the rate performance of the system, respectively.

Average information leakage rate is derived from fractional equivocation Δ and confidential information rate R_s, which is given by [4]

$$R_L = \mathbb{E}\{(1 - \Delta) R_s\}. \tag{5}$$

Therein, the fractional equivocation Δ characterizes the level at which the eavesdropper is confused [9] because of the dynamism of the wireless channel. Thus, the average information leakage rate tells how fast the information is leaked to the eavesdropper. In the fixed-rate on-off transmission system, (5) can be further derived as [4]

$$R_L = \frac{1}{\ln 2} \exp\left(\frac{1}{\bar{\gamma}_e}\right)\left(Ei\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - Ei\left(-\frac{2^{R_b - R_s}}{\bar{\gamma}_e}\right)\right), \tag{6}$$

where $Ei(x) = \int_{-\infty}^{x} \frac{\exp(t)}{t} dt$ is the exponential integral function. We can find that R_L is increasing on R_s and decreasing on R_b.

Throughput is a widely-adopted metric to measure the confidential information received by an intended user in a real-world communication system. In our system, the throughput is given by

$$\eta = p_{tx} R_s = \exp\left(-\frac{2^{R_b} - 1}{\bar{\gamma}_b}\right) R_s. \tag{7}$$

Note that η is increasing on R_s and decreasing on R_b.

D. Cases

To thoroughly understand the trade-off between throughput and information leakage rate, we consider the following two cases in secure transmission designs:

- **Case 1**: Maximizing throughput with average information leakage rate constraint is considered. This case represents the scenario where the throughput of the transmission is given the priority and the security is secondary to be considered.
- **Case 2**: Minimizing average information leakage rate with throughput constraint is considered. This case represents the scenario where the security of the wireless link is first taken into consideration and the throughput is subordinate.

The above two cases summarize many widely-used wireless communication services like video call and mobile payment in practice, thus are of great significance to consider.

III. System Design with Approximation

The implicit exponential integral function that is involved in average information leakage rate hinders the analytic analysis and incurs a high computation complexity in obtaining the optimal transmission rates of secure transmission. Although there are many existing works on approximations for the exponential integral function, none of them works in secure transmission designs directly. Consequently, an easy-to-evaluate approximation is desired for further research on the throughput-information leakage rate trade-off. To tackle this obstacle and examine the role of information leakage rate in wireless communication systems, in this section, we firstly propose a reasonable approximation for average information leakage rate. Subsequently, we detail optimal secure transmission design in the above two cases with the obtained approximation. At last, based on the approximation, analytical analysis is given at the end of each case.

A. Approximation for the Average Information Leakage Rate

To settle the obstacle brought by exponential integral function, we propose an approximation for average information leakage rate with the help of Abramowitz and Stegun's upper and lower bounds of $Ei(\cdot)$ [10] and classical Lagrange's mean value theorem [11]. We denote R_{Lp} as the approximation for R_L when $\bar{\gamma}_b$ is large. Note that large R_b will contribute to a high transmission rate of confidential information or high secrecy cost for preventing confidential information leaked. Thus, consideration of large R_b is of practical interest for the study on physical layer security. The approximation is summarized into the following proposition.

Proposition 1 *Approximation for the average information leakage rate, when $\bar{\gamma}_b$ is large, is given by*

$$R_{Lp} = \frac{3\bar{\gamma}_e \exp\left(\frac{1}{\bar{\gamma}_e}\right)}{10\ln 2}\,\frac{2^{R_s}-1}{2^{R_b}}. \tag{8}$$

Proof: See Appendix A. ■

As shown in (8), R_{Lp} is the simple combination of basic functions and does not involve the exponential integral function $Ei(\cdot)$, which makes it much easier to use and analyze. Based on the derived approximation, we can now derive the closed-form approximate optimal secure transmission rates in the following two different cases.

B. Approximate the Optimal Transmission Rates for Case 1

In Case 1, the system maximizing throughput subject to average information leakage rate constraint is considered, and the optimization problem is formulated as

$$\max_{R_b,R_s} \quad \eta = \exp\left(-\frac{2^{R_b}-1}{\bar{\gamma}_b}\right)R_s\,, \tag{9}$$

$$s.t. \quad R_L \le \xi\,,\ 0 \le R_s \le R_b, \tag{10}$$

where ξ is the maximum average information leakage rate permitted in this transmission system.

Problem reformulation. With the approximation in Proposition 1, an approximate optimization problem for Case 1 is obtained, which is given by

$$\max_{R_b,R_s} \quad \eta = \exp\left(-\frac{2^{R_b}-1}{\bar{\gamma}_b}\right)R_s\,, \tag{11}$$

$$s.t. \quad R_{Lp} \le \xi\,,\ 0 \le R_s \le R_b\,. \tag{12}$$

Feasibility of constraint ξ. To obtain the feasible range of ξ is equivalent to determine the maximum average information leakage rate. Given any R_b, we find that $\partial R_{Lp}/\partial R_s$ is more than 0. Hence given any R_b, it is wise to have maximum R_s, i.e., $R_s = R_b$, for maximizing R_{Lp}. Then by having R_b approaching $+\infty$, the upper bound of R_{Lp} is obtained. Thus, feasible range of ξ is given by

$$0 < \xi \le \frac{3\bar{\gamma}_e \exp\left(\frac{1}{\bar{\gamma}_e}\right)}{10\ln 2}. \tag{13}$$

Approximate optimal transmission rates. We denote $W_0(\cdot)$ as the principal branch of the Lambert W function and $A = \frac{10\ln 2\exp\left(-\frac{1}{\bar{\gamma}_e}\right)}{3\bar{\gamma}_e}$. The closed-form optimal secure transmission rates for the approximate optimization problem are summarized into the following proposition.

Proposition 2 *Approximate optimal transmission rates of the system maximizing throughput subject to average information leakage rate constraint are given by*

$$R_{s1}^{*} = \log_2\left(1+\xi A 2^{R_{b1}^{*}}\right) \tag{14}$$

and

$$R_{b1}^{*} = \max\left(R_{b1,min}\,,\ R_{b1,0}\right), \tag{15}$$

where

$$R_{b1,min} = -\log_2\left(1-\xi A\right) \tag{16}$$

and

$$R_{b1,0} = \log_2\left(\frac{\exp\left(W_0\left(\xi A\bar{\gamma}_b\right)\right)-1}{\xi A}\right). \tag{17}$$

Proof: See Appendix B. ■

Analysis based on Proposition 2. From Proposition 2, important observations could be obtained. When $\xi = 0$, we find that $R_{s1}^{*} = 0$, which implies no confidential information is transmitted if no information leakage is permitted. In this situation, the communication system is meaningless because only random noises is transmitted. Because $R_{b1,min}$ is increasing and $R_{b1,0}$ is decreasing with respect to ξ, respectively, $R_{b1,min}$ and $R_{b1,0}$ may encounter at a certain value of ξ, ξ_0, where ξ_0 is the solution of the equation $R_{b1,0} = R_{b1,min}$. When ξ exceeds ξ_0, we have $R_{b1}^{*} = R_{b1,min}$ and $R_{s1}^{*} = R_{b1}^{*}$, which leads to zero secrecy cost. In this situation, the secure system is incapable, for no confidential information is shield from the eavesdropper over the wireless channel. The observations reveals that both too stringent and too loose security constraints will result in impractical communication systems.

C. Approximate the Optimal Transmission Rates for Case 2

In Case 2, the system minimizing average information leakage rate subject to throughput constraint is taken into account. The optimization problem is formulated as

$$\min_{R_s,R_b} R_L = \frac{1}{\ln 2}\exp\left(\frac{1}{\bar{\gamma}_e}\right)\left(Ei\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - Ei\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right)\right), \quad (18)$$

$$s.t. \quad \eta \geq \Gamma\,,\ 0 \leq R_s \leq R_b\,, \quad (19)$$

where Γ represents the minimum throughput required in this transmission system.

Problem reformulation. With the approximation in Proposition 1, an approximate optimization problem for Case 2 is obtained, which is given by

$$\min_{R_s,R_b} \quad R_{Lp} = \frac{3\bar{\gamma}_e \exp\left(\frac{1}{\bar{\gamma}_e}\right)}{10\ln 2}\frac{2^{R_s}-1}{2^{R_b}}\,, \quad (20)$$

$$s.t. \quad \eta \geq \Gamma\,,\ 0 \leq R_s \leq R_b\,. \quad (21)$$

Feasibility of constraint Γ. For fixed R_b, we find that $\partial\eta/\partial R_s$ is always positive. Hence for fixed R_b, we have the maximum R_s, i.e., $R_s = R_b$, for maximizing η. Then, by solving the equation $\frac{\partial\eta(R_s=R_b)}{\partial R_b} = 0$, the R_b maximizing $\eta\left(R_s = R_b\right)$ is obtained, which is equal to $\frac{W_o(\bar{\gamma}_b)}{\ln 2}$. Thus, the feasible range of Γ is given by

$$0 \leq \Gamma \leq \frac{W_o(\bar{\gamma}_b)}{\ln 2}\exp\left(\frac{1-2^{\frac{W_o(\bar{\gamma}_b)}{\ln 2}}}{\bar{\gamma}_b}\right). \quad (22)$$

Approximate optimal transmission rates. We denote $R_{b2,min}$ and $R_{b2,max}$ as the solutions of x to $\exp\left(\frac{1-2^x}{\bar{\gamma}_b}\right)x = \Gamma$, where $R_{b2,min} < R_{b2,max}$. The optimal transmission rates for the approximate optimization problem are summarized into the following proposition.

Proposition 3 *Approximate optimal transmission rates of the system minimizing average information leakage rate subject to throughput constraint are given by*

$$R_{s2}^{*} = \Gamma\exp\left(\frac{2^{R_{b2}^{*}}-1}{\bar{\gamma}_b}\right) \quad (23)$$

and

$$R_{b2}^{*} = \begin{cases} R_{b2,min}\,, & if \quad R_{b2,0} < R_{b2,min}\,, \\ R_{b2,0}\,, & if \quad R_{b2,min} \leq R_{b2,0} \leq R_{b2,max}\,, \\ R_{b2,max}\,, & if \quad R_{b2,max} < R_{b2,0}\,, \end{cases} \quad (24)$$

where

$$R_{b2,0} = \log_2\left(1 + \bar{\gamma}_b \ln\left(\frac{\ln B}{\Gamma \ln 2}\right)\right) \quad (25)$$

and B is the solution of x to the equation

$$x\ln(x)\ln\left(\frac{1}{\Gamma\ln 2}\exp\left(\frac{1}{\bar{\gamma}_b}\right)\ln(x)\right) - x + 1 = 0\,. \quad (26)$$

Proof: See Appendix C. ■

Analysis based on Proposition 3. With the optimal secure transmission rates given in Proposition 3, insightful observations could be obtained. When $\Gamma = 0$, we have $R_{s2}^{*} = 0$, which implies that all the codeword transmission bits are leveraged to provide secrecy against the eavesdropper. In this situation, the system is unprofitable for no useful information is transmitted. When $\Gamma = \frac{W_o(\bar{\gamma}_b)}{\ln 2}$, we find that $R_{s2}^{*} = R_{b2}^{*}$, which demonstrates that the secrecy cost is maximum for any given R_b and all the codeword transmission bits are occupied by the confidential information. In this situation, the system is unsafe because no confidential information is shield from eavesdropping over the wireless channel. The observations also tell that both too stringent and too loose throughput constraint will make the communication system impractical.

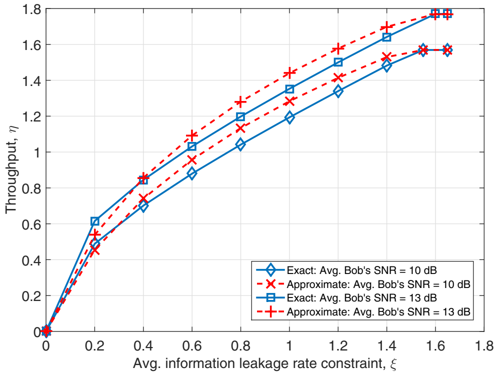

Fig. 1. : Throughput versus average information leakage rate constraint with $\bar{\gamma}_e$ = 3dB in Case 1.

IV. Numerical Results

In this section, we present the numerical results for wireless systems with $\bar{\gamma}_e$ = 3dB and different levels of $\bar{\gamma}_b$ to demonstrate the role of information leakage on secure transmission designs. In each figure, the exact curve is obtained by numerically solving the optimization problem (9) or (18), however, the approximate curve is obtained by Proposition 2 or 3.

We first present throughput versus security constraint subject to different levels of Bob's average SNR in Case 1. Fig. 1 shows that η is an upward convex non-decreasing function of ξ. And there exists a limitation on the throughput as the security constraint increases, which means much too loose security constraint does not contribute to higher throughput in this case. Another observation is that the system with a higher $\bar{\gamma}_b$ achieves higher throughput. But when the security constraint is very small, the difference in throughput between the systems is small. It is worth noting that the observations above are founded on both the exact and approximate curves. In addition, the maximum absolute error of the approximate curves with $\bar{\gamma}_b$ = 10dB and $\bar{\gamma}_b$ = 13dB are less than 0.2 and 0.1, respectively, which indicates the approximation of $Ei(\cdot)$ is reasonable in Case 1.

We then focus on secrecy cost versus security constraint for different systems in Case1. As depicted in Fig. 2, ϕ is a non-increasing function of ξ. And there exists a certain value, beyond which the secrecy cost equals zero as the security constraint increases. This observation confirms our

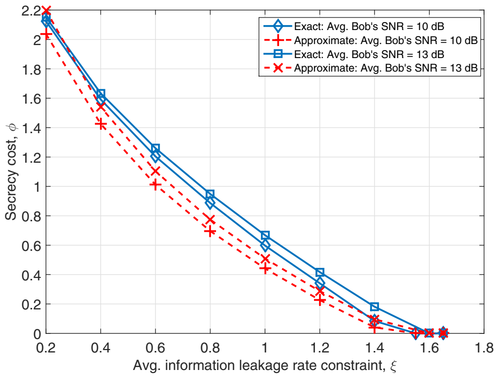

Fig. 2. : Transmission rates versus average information leakage rate constraint with $\bar{\gamma}_b$ = 13dB and $\bar{\gamma}_e$ = 3dB in Case 1.

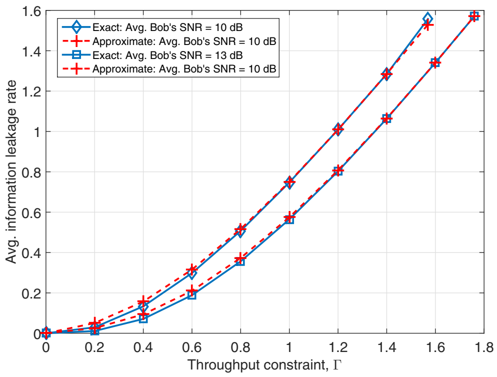

Fig. 3. : Average information leakage rate versus throughput constraint with $\bar{\gamma}_e$ = 3dB in Case 2.

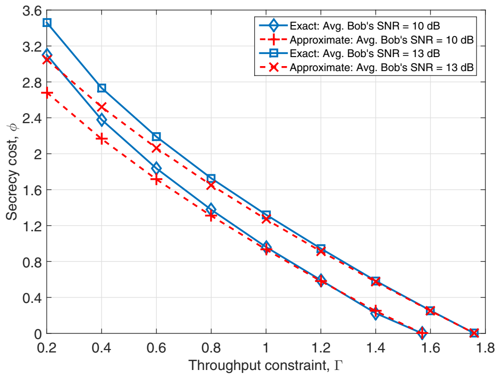

Fig. 4. : Transmission rates versus throughput constraint with $\bar{\gamma}_b$ = 13dB and $\bar{\gamma}_e$ = 3dB in Case 2.

analytic analysis that when ξ exceeds ξ_0, $R_{s1}^* = R_{b1}^*$. We also find that the system with better main channel quality pays a higher secrecy cost against eavesdropping. We can see these observations found on both the exact and approximate curves. Additionally, the maximum absolute distances between the exact and approximate curves with $\bar{\gamma}_b$ = 10dB and $\bar{\gamma}_b$ = 13dB are less than 0.25 and 0.2, respectively.

Next, we illustrate average information leakage rates versus throughput constraint subject to different levels of Bob's average SNR in Case 2. As shown in Fig. 3, average information leakage rate is a lower convex increasing function of Γ. However, there is no limitation on information leakage rate like throughput in Case 1. We also observed that the system with a higher $\bar{\gamma}_b$ has a lower average information leakage rate. However, when the throughput constraint is very small, the difference in average information leakage rate between the systems is small. Note that the maximum absolute error of R_{Lp} with $\bar{\gamma}_b$ = 10dB and $\bar{\gamma}_b$ = 13dB are less than 0.1 and 0.05, respectively, which indicates the approximation is reasonable in Case 2, too.

Finally, we show secrecy cost versus throughput constraint for different communication systems in Case 2. As depicted in Fig. 4, the secrecy cost decreases as the throughput constraint increases. And the secrecy cost goes to zero at the upper bound of the throughput constraint. The observation testifies our analytical analysis that when $\Gamma = \frac{W_o(\bar{\gamma}_b)}{\ln 2}$, $R_{s2}^* = R_{b2}^*$. We also observe that the system with a high average main channel SNR obtains more secrecy cost for more random noises in the codeword transmission rate needed to disturbing the eavesdropper for secure transmission. Note that the maximum absolute distances between exact and approximate curves in two systems are both less than 0.4.

V. Conclusion

In this work, we investigate secure transmission designs from an information leakage perspective. Specifically, to address the obstacle brought by exponential integral function, we proposed a reasonable approximation for average information leakage rate. Based on the proposed approximation, the optimal transmission rates in two cases are obtained, respectively. Through analytical and numerical results, we found that for the system maximizing throughput subject to information leakage rate constraint, the throughput is an upward convex non-decreasing function of the security constraint. However, for the system minimizing information leakage rate subject to throughput constraint, the average information leakage rate is a lower convex increasing function of the throughput constraint. Additionally, in each case, a higher average Bob's SNR contributes to better throughput or security performance over the wireless channel. It is worth noting that all insightful observations are found on both the exact and approximate curves and the maximum absolute error in all figures are low, which testifies the proposed approximation is reasonable. Altogether, these results provide some important insights on information leakage in secure transmission designs.

Appendix A
Proof of Proposition 1

From $R_L = \frac{1}{\ln 2}\exp\left(\frac{1}{\bar{\gamma}_e}\right)\left(Ei\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - Ei\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right)\right)$, we find that to approximate R_L is mainly to approximate

$$O = Ei\left(-\frac{x}{\bar{\gamma}_e}\right) - Ei\left(-\frac{x}{\bar{\gamma}_e y}\right), \tag{27}$$

where x and y denote 2^{R_b} and 2^{R_s}, for simplicity, respectively. With Abramowitz and Stegun's bounds of $Ei(\cdot)$ [10], we have

$$O \approx -\frac{1}{2}\exp\left(-\frac{x}{\bar{\gamma}_e}\right)\ln\left(1+\frac{2\bar{\gamma}_e}{x}\right)+\exp\left(-\frac{x}{\bar{\gamma}_e y}\right)\ln\left(1+\frac{\bar{\gamma}_e y}{x}\right). \tag{28}$$

With infinitesimal equivalence, $\ln\left(1+\frac{2\bar{\gamma}_e}{x}\right) \approx \frac{2\bar{\gamma}_e}{x}$ and $\ln\left(1+\frac{\bar{\gamma}_e y}{x}\right) \approx \frac{\bar{\gamma}_e y}{x}$ when $\bar{\gamma}_b$ is large. By doing the corresponding equivalence infinitesimal replacement in (28), we have

$$\begin{aligned} O \approx& -\frac{1}{2}\exp\left(-\frac{x}{\bar{\gamma}_e}\right)\frac{2\bar{\gamma}_e}{x}+\exp\left(-\frac{x}{\bar{\gamma}_e y}\right)\frac{\bar{\gamma}_e y}{x} \\ =&\frac{\bar{\gamma}_e}{x}\left(y\exp\left(-\frac{x}{\bar{\gamma}_e y}\right)-\exp\left(-\frac{x}{\bar{\gamma}_e}\right)\right) \\ =&\bar{\gamma}_e\frac{y-1}{x}\left(\frac{y\exp\left(-\frac{x}{\bar{\gamma}_e y}\right)-\exp\left(-\frac{x}{\bar{\gamma}_e}\right)}{y-1}\right). \end{aligned} \tag{29}$$

We denote $f(z) = z\exp\left(-\frac{x}{\bar{\gamma}_e z}\right)$ and $f(z)$ with respect to z is continuous and differentiable on closed interval $[1, y]$. From Lagrange's mean value theorem [11], there exists a point c in $(1\ ,\ y)$ such that $f^{'}(c) = \frac{f(y)-f(1)}{y-1}$. Hence, we have

$$O \approx f^{'}(c)\bar{\gamma}_e\frac{y-1}{x}. \tag{30}$$

Besides, when $1 \le x \le \infty$ and $1 \le z \le x$, we have $0 < f^{'}(z) < 1$. By setting $\alpha = f^{'}(c)$, we obtain

$$O \approx \alpha\bar{\gamma}_e\frac{y-1}{x}, \tag{31}$$

where $\alpha \in (0\ ,\ 1)$. To reduce computational complexity in our problem, we empirically set $\alpha = 3/10$, which provides good accuracy. Recalling that $x = 2^{R_b}$ and $y = 2^{R_s}$, we have the approximation in (8). This completes the proof.

Appendix B
Proof of Proposition 2

From the constraint condition $R_{Lp} \le \xi$, we have

$$R_s \le \log_2\left(1+\xi A 2^{R_b}\right). \tag{32}$$

Given any R_b, we find that $\partial\eta/\partial R_s$ is always more than 0. Hence given any R_b, it is wise to have the maximum R_s, i.e., $R_s = \log_2\left(1+\xi A 2^{R_b}\right)$, for maximizing η. Thus, R_{s1}^{*} is obtained in (14). Additionally, with $R_s = \log_2\left(1+\xi A 2^{R_b}\right)$ and $R_s \le R_b$, the feasible range of R_b is given by

$$R_{b1,min} = -\log_2(1-\xi A) \le R_b. \tag{33}$$

Then, we can rewrite the optimization problem as

$$\max_{R_b} \quad \eta|_{R_s=\log_2\left(1+\xi A 2^{R_b}\right)}\ , \tag{34}$$

$$s.t \quad R_{b1,min} \le R_b\ . \tag{35}$$

Finally, by solving for R_s in the equation $\frac{\partial\eta(R_b)}{\partial R_b} = 0$, the only maximum value point $R_{b1,0}$ can be obtained in (17). Hence, R_{b1}^{*} is obtained in (15). This completes the proof.

Appendix C
Proof of Proposition 3

From the constraint condition $\eta \ge \Gamma$, we have

$$R_s \ge \Gamma\exp\left(\frac{2^{R_b}-1}{\bar{\gamma}_b}\right). \tag{36}$$

Given any R_b, we find that $\partial R_{Lp}/\partial R_s$ is always more than 0. Hence given any R_b, it is wise to have the minimum R_s, i.e., $R_s = \Gamma\exp\left(\frac{2^{R_b}-1}{\bar{\gamma}_b}\right)$, for minimizing R_{Lp}. Thus, R_{s2}^{*} is given in (23).

Then, as analyzed in obtaining the feasibility of Γ, given any R_b, it is wise to have the maximum R_s, i.e., $R_s = R_b$, for maximizing η. Hence, we can obtain the feasible range of R_b for satisfying the throughput constraint by solving R_s in the equation $\eta(R_s = R_b) = \Gamma$. The feasible range is given by

$$R_{b2,min} \le R_b \le R_{b2,max}. \tag{37}$$

Consequently, the optimization problem can be rewrite as

$$\min_{R_b} \quad R_{Lp}|_{R_s=\Gamma\exp\left(\frac{2^{R_b}-1}{\bar{\gamma}_b}\right)}\ , \tag{38}$$

$$s.t. \quad R_{b2,min} \le R_b \le R_{b2,max}\ . \tag{39}$$

Finally, the minimum value point $R_{b2,0}$ can be obtained by solving for R_b in the equation $\frac{\partial R_{Lp}(R_b)}{\partial R_b} = 0$. We find that the closed-form solution of $R_{b2,0}$ is mathematically intractable. We can numerically obtain $R_{b2,0}$ by (25) and (26). Thus, R_{b2}^{*} is given in (24). This completes the proof.

Acknowledgement

The research was supported in part by the National Science Foundation of China under Grant 61502114, 91738202 and 61729101, the National Natural Science Foundation of China through grant 61671003, as well as the Fundamental Research Funds for the Central Universities with grand HUST: 2018JYCXJJ031 and YWF-18-BJ-Y-176.

References

[1] W. Wang, L. Yang, Q. Zhang, and T. Jiang, "Securing on-body IoT devices by exploiting creeping wave propagation," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, 2018.

[2] W. Wang, L. Yang, and Q. Zhang, "Resonance-based secure pairing for wearables," *IEEE Transactions on Mobile Computing*, 2018.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6913–6924, 2016.

[5] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Communications Letters*, 2017.

[7] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, 2011.

[8] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1923–1936, 2013.

[9] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[10] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, vol. 55.

[11] W. Rudin, "Principles of mathematical analysis (international series in pure & applied mathematics)," 1976.