New Physical Layer Security Measures for Wireless Transmissions over Fading Channels

Biao He and Xiangyun Zhou
Research School of Engineering, The Australian National University, Australia
Email: biao.he@anu.edu.au, xiangyun.zhou@anu.edu.au

***Abstract*—For secure communications over wireless fading channels, the secrecy outage probability is widely used as the performance measure. However, the current secrecy outage formulation has two major limitations in evaluating the secrecy performance: a) the amount of information leakage to the eavesdropper cannot be characterized when an outage occurs, b) the current formulation does not give insights into the eavesdropper's decodability of confidential messages. To overcome such limitations and obtain in-depth understanding of secrecy performance over wireless fading channels, this paper proposes three new secrecy measures for different practical aims, namely, 1) generalized secrecy outage probability, 2) asymptotic lower bound on eavesdropper's decoding error probability, and 3) average information leakage rate. A specific example of wireless transmissions with a fixed-rate wiretap code is given to illustrate the use of the proposed secrecy measures.**

I. Introduction

Physical layer security has been widely regarded as a complement to cryptographic technologies for providing the wireless communication security in future networks [1, 2]. Recent development on physical layer security over wireless fading channels has paid increasing attention to the scenarios where the eavesdropper's instantaneous channel state information (CSI) is not known to legitimate users, e.g., [3] and references therein. The secrecy performance in such scenarios is often characterized by either ergodic secrecy capacity [4] or secrecy outage probability [5, 6]. For the transmission over fast fading channels, the ergodic secrecy capacity characterizes the capacity limit subject to the constraint of perfect secrecy. For the transmission over quasi-static fading channels where perfect secrecy is not always achievable, the secrecy outage formulation measures the probability of failing to achieve perfect secrecy. Here perfect secrecy means that the amount of information leakage to the eavesdropper vanishes. It guarantees that the eavesdropper's optimal attack is to guess the message at random, and hence the eavesdropper's decoding error probability, P_e, asymptotically goes to 1.

However, the current formulation of secrecy outage probability has two major limitations in evaluating the secrecy performance of wireless systems where perfect secrecy is not always achievable.

a) The amount of information leakage to the eavesdropper cannot be characterized. When perfect secrecy is not always achievable, some information would be leaked to the eavesdropper. Then, it is important to know how much or how fast the confidential information is leaked to the eavesdropper. However, the current outage-based approach is not able to evaluate the amount of information leakage when a secrecy outage occurs.
b) The current secrecy outage probability does not give insights into the eavesdropper's decodability of confidential messages. In fact, the secrecy performance is also commonly interpreted in terms of the eavesdropper's decoding error probability, e.g., [7–9]. Generally, a secrecy requirement can be given as $P_e \geq \epsilon$, where $0 < \epsilon \leq 1$ denotes the minimum acceptable value of P_e. The current secrecy outage probability only reflects an extremely stringent requirement on P_e for $\epsilon = 1$, since perfect secrecy guarantees $P_e \to 1$. Therefore, the outage definition needs to be generalized in order to reflect different secrecy requirements in terms of P_e for $0 < \epsilon \leq 1$.

Apart from the perfect secrecy regime, there exists another regime of interest in physical layer security, namely the partial secrecy regime. The partial secrecy of transmission is often investigated by the equivocation that reflects the level at which the eavesdropper is confused. The exploration on equivocation can be found as early as Wyner's pioneering work for the wiretap channel [10]. Similarly, Csiszár and Körner [11] used the normalized equivocation to quantify the partial secrecy for the broadcast channel with confidential information. In addition, the equivocation is related to the decoding error probability [10, 12, 13], which confirms that evaluating security on the basis of equivocation is related to the conventional requirement of a decoding error probability at the eavesdropper.

In this work, we propose new secrecy measures for wireless transmissions by applying the existing results on partial secrecy to the case of quasi-static fading channels. For different practical aims, three performance measures are proposed:

1) Extending the current definition of secrecy outage, a generalized formulation of secrecy outage probability is proposed. The generalized secrecy outage probability takes into account the level of secrecy requirement measured by equivocation, and hence is applicable for networks with different levels of secrecy requirements in terms of the decodability of messages at the eavesdropper.
2) An asymptotic lower bound on eavesdropper's decoding error probability is proposed. Although the eavesdropper's exact decoding error probability cannot be directly characterized, the proposed measure gives a worst-case estimation of eavesdropper's decodability.
3) A measure evaluating the average information leakage rate is proposed. When perfect secrecy is not always achiev-

978-1-4799-3512-3/14/$31.00 ©2014 IEEE

able, it is important to know how fast or how much the confidential information is leaked to the eavesdropper. The proposed measure provides answers to these important questions.

The newly proposed metrics can be used to obtain more comprehensive and in-depth understanding of physical layer security performance over wireless fading channels.

The remainder of this paper is organized as follows. Section II gives the preliminary on perfect secrecy and partial secrecy. Section III introduces our main results, i.e., the three new secrecy measures for wireless systems where perfect secrecy is not always achievable. Section IV demonstrates how to evaluate the secrecy performance by the proposed secrecy measures in a specific example of wireless transmissions with a fixed-rate wiretap code. Finally, Section V concludes the paper.

II. Preliminary on Perfect Secrecy and Partial Secrecy

Consider a basic system that a transmitter, Alice, wants to send confidential information, M, to an intended user, Bob, in the presence of an eavesdropper, Eve. The source is stationary and ergodic. The confidential information, M, is encoded into a n-vector X^n. The received vectors at Bob and Eve are Y^n and Z^n, respectively. The entropy of the source information and the residual uncertainty for the message at the eavesdropper are given by $H(M)$ and $H(M \mid Z^n)$, respectively.

A. Perfect Secrecy

As mentioned before, perfect secrecy means that the amount of information leakage to the eavesdropper vanishes, and guarantees that the eavesdropper's optimal attack is to guess the message at random. From Shannon's definition, perfect secrecy requires the statistical independence between messages and Eve's observations, which is given by

$$H(M \mid Z^n) = H(M) \quad \text{or, equivalently,} \quad I(M, Z^n) = 0. \tag{1}$$

Since Shannon's definition of perfect secrecy is not convenient to be used for further analysis, current researches often investigate the strong secrecy or weak secrecy. Strong secrecy requires asymptotic statistical independence of the message and Eve's observation as the codeword length goes to infinity, i.e., $\lim_{n\to\infty} I(M, Z^n) = 0$. Weak secrecy requires that only the rate of information leaked to the eavesdropper vanishes, i.e, $\lim_{n\to\infty} \frac{1}{n} I(M, Z^n) = 0$. Since strong secrecy, weak secrecy and Shannon's perfect secrecy all belong to the perfect secrecy regime, for simplicity, we use the term "perfect secrecy" to refer to such a regime in this paper.[1]

The requirement of no information leakage to Eve in fact is equivalent to guaranteeing the highest possible decoding error probability at Eve. As explained in [1, Remark 3.1], consider that messages are uniformly taken from a size K set $[1, 2, \cdots, K]$, and Eve minimizes her decoding error probability P_e by performing maximum-likelihood decoding. The condition of no information leakage ensures that Eve can only guess the original message, and the probability of error under maximum-likelihood decoding is $P_e = \frac{K-1}{K}$. Therefore, from the decodability point of view, perfect secrecy is equivalent to guaranteeing $P_e \geq \frac{K-1}{K}$. Furthermore, when the entropy of the message is very large that $K \to \infty$, perfect secrecy actually guarantees that P_e asymptotically goes to 1,

$$\lim_{K\to\infty} P_e \geq \lim_{K\to\infty} \frac{K-1}{K} = 1. \tag{2}$$

In practice, the secrecy requirement on the decodability of messages at Eve can be generally written as $P_e \geq \epsilon$ for some ϵ. Depending on the applications, the value of ϵ ranges from 0 to 1, which falls outside the perfect secrecy regime.

B. Partial Secrecy

The partial secrecy of transmissions is often investigated by the equivocation that indicates the level at which Eve is confused. In this paper, we specifically consider the fractional equivocation, which is defined by [14]

$$\Delta = \frac{H(M \mid Z^n)}{H(M)}. \tag{3}$$

Note that evaluating security on the basis of equivocation is related to the conventional requirement on the decodability of messages at Eve [10]. Although there is no one-to-one relation between the equivocation and the error probability, the tight lower and upper bounds of the decoding error probability can be derived from the equivocation [12, 13].

Specifically, when considering secrecy issues, we want to ensure that the decoding error probability at eavesdropper is larger than a certain level. Thus, it is desirable to have the decoding error probability at Eve lower bounded by the equivocation. Still consider the general case where messages are uniformly taken from a size K set $[1, 2, \cdots, K]$, which achieves the maximal entropy over an alphabet of size K. Then, the entropy of the message is given by $H(M) = \log_2(K)$. From fano's inequality [12, Chapter 2.10], we have

$$H(M \mid Z^n) \leq h(P_e) + P_e \log_2(K), \tag{4}$$

where $h(x) = -x \log_2(x) - (1-x)\log_2(1-x),\ 0 \leq x \leq 1$. This inequality can be weakened to

$$P_e \geq \frac{H(M \mid Z^n) - 1}{\log_2(K)} = \Delta - \frac{1}{\log_2(K)}. \tag{5}$$

When the entropy of the message is very large that $K \to \infty$, we can further derive (5) as

$$\lim_{K\to\infty} P_e \geq \Delta - \lim_{K\to\infty} \frac{1}{\log_2(K)} = \Delta. \tag{6}$$

III. New Secrecy Performance Measures for Wireless Transmissions

In this section, the main results of this work are presented. Keeping the basic system introduced in last section, we further assume that both Bob and Eve's channels are quasi-static fading channels. Bob and Eve perfectly know their own channels. However, Alice does not know Eve's instantaneous channel information.

[1] Also, for simplicity, we do not specify the assumption of $n \to \infty$ for the discussions in the rest of this paper.

For transmissions in such a network over quasi-static fading channels, perfect secrecy is not always achievable, and the outage-based formulation is commonly used to measure the secrecy performance. From the perfect secrecy perspective, the existing outage-based formulation treats the failure of achieving *perfect secrecy* as the case of secrecy outage. Thus, the existing secrecy outage formulation is applicable only for the system which has an extremely stringent requirement on Eve's decoding error probability, $\epsilon = 1$, but cannot handle the general requirement on Eve's decoding error probability, $0 < \epsilon \leq 1$. In addition, the existing outage-based formulation cannot evaluate how fast or how much the confidential information is leaked to Eve.

Different from the existing secrecy outage probability, we study the secrecy performance of wireless communications from the partial secrecy perspective. In wireless communications, the fractional equivocation, Δ, is a random variable due to the fading properties of channels. Thus, we start from the derivation of Δ for a given fading realization, and then the distribution of Δ can be obtained according to the distribution of channel gains. After that, three performance measures are proposed based on the distribution of Δ.

A. Fractional Equivocation for a Given Fading Realization

A given fading realization of the wireless channel is equivalent to the (non-degraded) Gaussian wiretap channel [15]. The value of the fractional equivocation for the Gaussian wiretap channel actually depends on the coding and transmission strategies, and there is no such a general expression applicable for all scenarios. However, an upper bound on Δ can be derived as follows.

Proposition 1: For a given fading realization of the wireless channel, the achievable fractional equivocation can be written as

$$\Delta \leq \begin{cases} 1 & \text{if} \quad C_e \leq C_b - R, \\ (C_b - C_e)/R & \text{if} \quad C_b - R < C_e < C_b, \\ 0 & \text{if} \quad C_b \leq C_e, \end{cases} \tag{7}$$

where C_b and C_e are Bob and Eve's channel capacities, respectively, $R = \frac{H(M)}{n}$ is the secrecy rate for transmission.

The proof follows closely from [15, Lemma 1 & Corollary 2] and [14, Theorem 1].

B. Proposed Secrecy Measures

Considering the fading properties of wireless channels, the distribution of Δ can be derived according to the distribution of channel gains. Then, we investigate the distribution of Δ from the following three aspects to propose three secrecy performance measures for different practical aims.

1) Generalized Secrecy Outage Probability:
Extending from the current perfect secrecy outage formulation, we propose a generalized definition of secrecy outage probability, given by

$$p_{\text{out}} = \Pr(\Delta < \theta), \tag{8}$$

where $\Pr(\cdot)$ denotes the probability measure and $0 < \theta \leq 1$ denotes the minimum acceptable value of the fractional equivocation.

Since the fractional equivocation is related to the decoding error probability, the new outage formulation is applicable for systems with different levels of secrecy requirements in terms of Eve's decodability of confidential messages (by choosing different values of θ). The existing secrecy outage probability is defined as $\Pr(\Delta < 1)$, and hence is a special case of the newly proposed secrecy outage probability (by setting $\theta = 1$).

Apart from the discussion above, another way to understand the generalized secrecy outage probability can be described as follows. From (3), the information leakage ratio to Eve can be written as $\frac{I(M,Z^n)}{H(M)} = 1 - \Delta$. Then, the generalized secrecy outage probability, $p_{\text{out}} = \Pr(\Delta < \theta) = \Pr(1 - \Delta > 1 - \theta)$, actually characterizes the probability that the information leakage ratio is larger than a certain value, $1 - \theta$.

2) Average Fractional Equivocation – Asymptotic Lower Bound on Eavesdropper's Decoding Error Probability:
Taking average of the fractional equivocation from its distribution, we can derive the (long-term) average value of the factional equivocation, given by

$$\bar{\Delta} = E\{\Delta\}, \tag{9}$$

where $E\{\cdot\}$ denotes the expectation operation. As discussed earlier, when the entropy of message for transmission is very large, Eve's decoding error probability for a given fading realization is lower bounded by the fractional equivocation. Thus, the average factional equivocation, $\bar{\Delta}$, actually gives an asymptotic lower bound on the overall decoding error probability at Eve, i.e, $P_e \geq \bar{\Delta}$.

3) Average Information Leakage Rate:
With the knowledge of message transmission rate $R = \frac{H(M)}{n}$, we can further derive the average information leakage rate, given by

$$\begin{aligned} R_L &= E\left\{\frac{I(M,Z^n)}{n}\right\} \\ &= E\left\{\frac{I(M,Z^n)}{H(M)} \cdot \frac{H(M)}{n}\right\} \\ &= E\left\{(1-\Delta)R\right\}. \end{aligned} \tag{10}$$

The average information leakage rate can tell us how fast the information is leaked to the eavesdropper. Note that the transmission rate R cannot be simply taken out of the expectation in (10), since R can be a variable parameter (e.g., adaptive-rate transmission) and its distribution may be correlated with the distribution of Δ. However, when the fixed-rate transmission scheme is adopt, (10) can be simplified as

$$R_L = E\left\{(1-\Delta)R\right\} = R_s \cdot (1 - \bar{\Delta}). \tag{11}$$

Remark: The proposed secrecy measures in this section, i.e., (8), (9) and (10), are general and can be applied to evaluate the performance of any coding and transmission strategy in any system model (e.g., signal-antenna or multi-antenna systems). A specific scenario is studied as an example in next section, wherein the expressions of proposed secrecy measures are further derived in terms of the transmission rate and channel statistics.

IV. Wireless Transmissions with a Fixed-Rate Wiretap Code: An Example

In this section, we present a specific example for illustrating how to compute the proposed secrecy measures in a given scenario.

A. System Model

We consider the system where a transmitter, Alice, wants to send confidential information to an intended receiver, Bob, in the present of an eavesdropper, Eve, over quasi-static Rayleigh-fading channels. Alice, Bob and Eve are assumed to have a single antenna each. Then, the instantaneous channel capacity at Bob or Eve can be written as

$$C_i = \log_2(1+\gamma_i), \quad i = b \text{ or } e, \tag{12}$$

where $\gamma_i > 0$ denotes the instantaneous signal-to-noise ratio (SNR), the subscripts b and e denote the parameters for Bob and Eve, respectively. The instantaneous SNR has an exponential distribution, given by

$$f_{\gamma_i}(\gamma_i) = \frac{1}{\bar{\gamma}_i}\exp\left(-\frac{\gamma_i}{\bar{\gamma}_i}\right), \quad i = b \text{ or } e, \tag{13}$$

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

We consider the widely-adopted wiretap code [10] for confidential message transmissions. There are two rate parameters, namely, the codeword transmission rate, $R_b = \frac{H(X^n)}{n}$, and the confidential information rate, $R_s = \frac{H(M)}{n}$. The positive rate difference $R_e = R_b - R_s$ is the cost to provide secrecy against the eavesdropper. A length n wiretap code is constructed by generating 2^{nR_b} codewords $x^n(w,v)$ of length n, 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 $\{1, 2, \cdots, 2^{n(R_b-R_s)}\}$ with uniform probability and transmit the codeword $x^n(w,v)$. In addition, we consider the fixed-rate transmission,[2] where the transmission rates, R_b and R_s, are fixed over time.

Bob and Eve perfectly know their own channels. Hence, the values of C_b and C_e are known at Bob and Eve, respectively. Alice has no knowledge about either Bob or Eve's instantaneous CSI. However, Bob provides one-bit feedback to Alice to enable an on-off transmission scheme [6], which guarantees that the transmission takes place only when $R_b \le C_b$.

B. Fractional Equivocation for a Given Fading Realization

To characterize the secrecy performance of wireless transmissions, we start from the investigation on a given fading realization of the wireless channel. The factional equivocation for the wiretap code of $R_b \le C_b$ and $R_s \le R_b$ is given as follows.

Corollary 1: For a given fading realization of the wireless channel, the achievable fractional equivocation for the wiretap code of $R_b \le C_b$ and $R_s \le R_b$ can be written as

$$\Delta = \begin{cases} 1 & \text{if} \quad C_e \le R_b - R_s, \\ (R_b - C_e)/R_s & \text{if} \quad R_b - R_s < C_e < R_b, \\ 0 & \text{if} \quad R_b \le C_e. \end{cases} \tag{14}$$

[2]Fixed-rate transmissions are often adopted to reduce complexity of the system. In practice, applications like video streams in multimedia often require fixed-rate transmissions.

The proof follows closely from [15, Lemma 1 & Corollary 2] and the steps in [14, Section III] while having $\frac{H(X^n)}{n} = R_b$.

From (12), we can further derive (14) as

$$\Delta = \begin{cases} 1 & \text{if} \quad \gamma_e \le 2^{R_b-R_s}-1, \\ \frac{R_b-\log_2(1+\gamma_e)}{R_s} & \text{if} \quad 2^{R_b-R_s}-1 < \gamma_e < 2^{R_b}-1, \\ 0 & \text{if} \quad 2^{R_b}-1 \le \gamma_e. \end{cases} \tag{15}$$

C. Secrecy Performance over Fading Channels

Now, we are ready to evaluate the secrecy performance over fading channels from the distribution of Δ according to the distribution of γ_e given in (13).

1) Generalized Secrecy Outage Probability:
The generalized secrecy outage probability is given by

$$\begin{aligned} p_{\text{out}} &= \Pr(\Delta < \theta) \\ &= \Pr\left(2^{R_b}-1 \le \gamma_e\right) + \Pr\left(2^{R_b-R_s}-1 < \gamma_e < 2^{R_b}-1\right) \\ &\quad \cdot \Pr\left(\frac{R_b-\log_2(1+\gamma_e)}{R_s} < \theta \,\middle|\, 2^{R_b-R_s}-1 < \gamma_e < 2^{R_b}-1\right) \\ &= \exp\left(-\frac{2^{R_b-\theta R_s}-1}{\bar{\gamma}_e}\right), \end{aligned} \tag{16}$$

where $0 < \theta \le 1$. For the extreme case of $\theta = 1$, we have

$$p_{\text{out}}(\theta = 1) = \exp\left(-\frac{2^{R_b-R_s}-1}{\bar{\gamma}_e}\right). \tag{17}$$

Note that (17) is exactly the same as [6, Eq. (8)], which gives the perfect secrecy outage probability of wireless transmissions with a fixed-rate wiretap code.

2) Average Fractional Equivocation – Asymptotic Lower Bound on Eavesdropper's Decoding Error Probability:
The average fractional equivocation is given by

$$\begin{aligned} \bar{\Delta} &= E\{\Delta\} \\ &= \int_0^{2^{R_b-R_s}-1} f_{\gamma_e}(\gamma_e)\mathrm{d}\gamma_e + \int_{2^{R_b-R_s}-1}^{2^{R_b}-1} \left(\frac{R_b-\log_2(1+\gamma_e)}{R_s}\right) f_{\gamma_e}(\gamma_e)\mathrm{d}\gamma_e \\ &= 1 - \frac{1}{R_s \ln 2}\exp\left(\frac{1}{\bar{\gamma}_e}\right)\left(\mathrm{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \mathrm{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right)\right), \end{aligned} \tag{18}$$

where $\mathrm{Ei}(x) = \int_{-\infty}^{x} e^t/t \ \mathrm{d}t$ is the exponential integral function. In addition, the average fractional equivocation actually gives an asymptotic lower bound on eavesdropper's decoding error probability.

3) Average Information Leakage Rate:
Since the fixed-rate transmission scheme is adopted, the average information leakage rate can be derived from (11), given by

$$\begin{aligned} R_L &= R_s \cdot (1 - \bar{\Delta}) \\ &= \frac{1}{\ln 2}\exp\left(\frac{1}{\bar{\gamma}_e}\right)\left(\mathrm{Ei}\left(-\frac{2^{R_b}}{\bar{\gamma}_e}\right) - \mathrm{Ei}\left(-\frac{2^{R_b-R_s}}{\bar{\gamma}_e}\right)\right), \end{aligned} \tag{19}$$

which captures how fast on average the information is leaked to Eve.

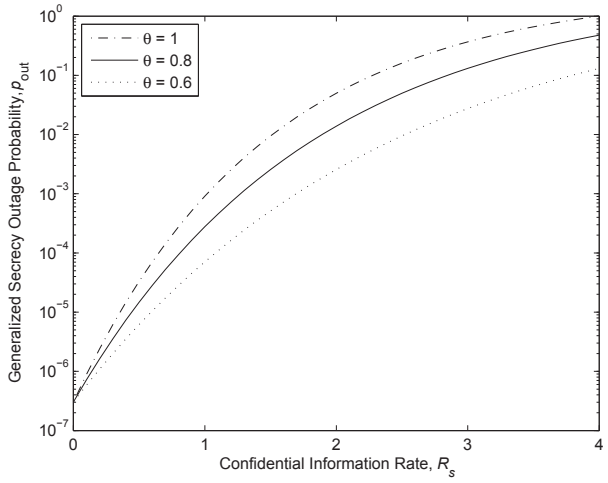

Fig. 1. Generalized secrecy outage probability versus confidential information rate. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8, 0.6$. The other parameters are $R_b = 4$ and $\bar{\gamma}_e = 1$.

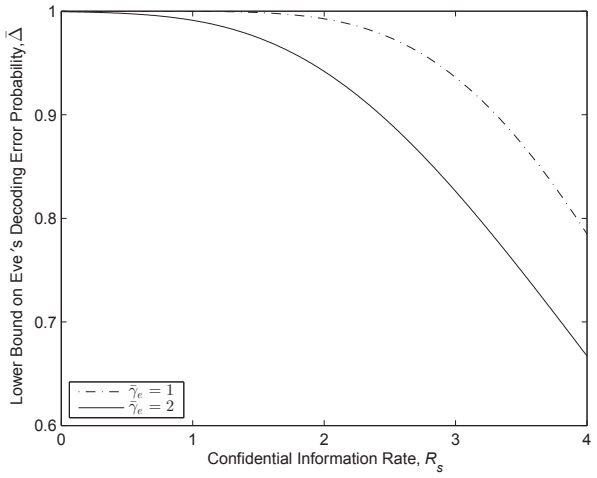

Fig. 3. Asymptotic lower bound on the decoding error probability at Eve versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\bar{\gamma}_e = 1, 2$. The other parameter is $R_b = 4$.

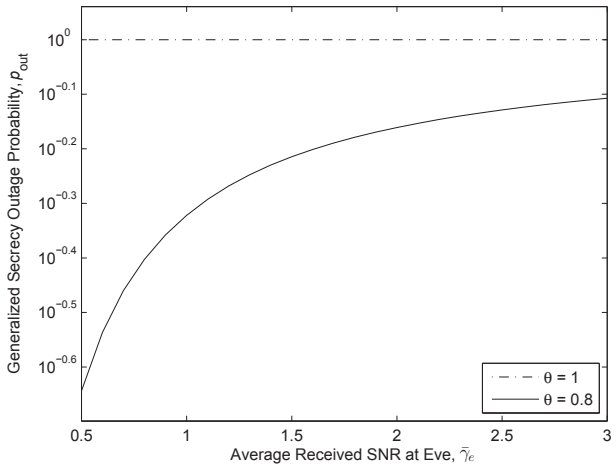

Fig. 2. Generalized secrecy outage probability versus average received SNR at Eve. Results are shown for networks with different requirements on the fractional equivocation, $\theta = 1, 0.8$. The other parameters are $R_b = R_s = 4$.

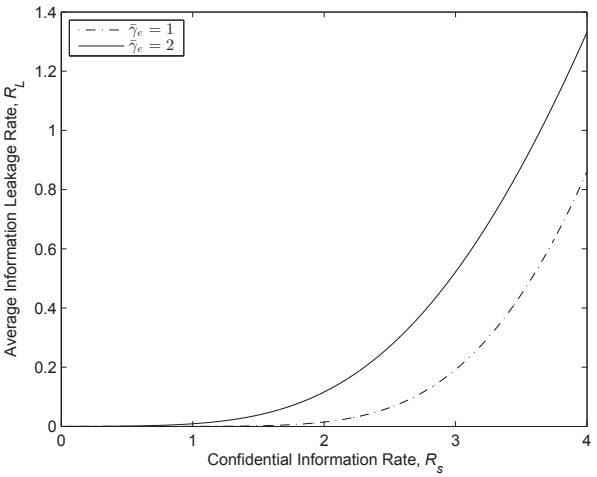

Fig. 4. Average information leakage rate versus confidential information rate. Results are shown for networks with different average received SNRs at Eve, $\bar{\gamma}_e = 1, 2$. The other parameter is $R_b = 4$.

D. Numerical Results

In this subsection, we illustrate numerical results on the proposed secrecy measures.

Figure 1 compares the secrecy outage performances of networks subject to different requirements on the fractional equivocation. Note that $\theta = 1$ represents the case of requiring perfect secrecy. As shown in the figure, for different levels of secrecy requirements in terms of the fractional equivocation or the decodability of messages at Eve, the transmission has different secrecy outage performances. In addition, when the confidential information rate is very small, the difference in outage probability between networks subject to different requirements on the fractional equivocation is small, and the difference increases as the confidential information rate increases.

Figure 2 compares the secrecy performances of transmissions measured by the existing perfect secrecy outage probability ($\theta = 1$) and the newly proposed generalized secrecy outage probability with[3] $\theta = 0.8$. We consider an extreme case that the confidential information rate is set to be the same as the total codeword rate, $R_b = R_s$. This is equivalent to using an ordinary code instead of the wiretap code for transmission. As shown in the figure, the secrecy performance measured by the perfect secrecy outage probability is not related to Eve's channel condition, since the perfect secrecy outage probability is always equal to 1. However, we know that the decodability of messages at the receiver is related to the channel condition. Intuitively, with the increase of average

[3]For generalized secrecy outage probability, we can choose any value of $0 < \theta \leq 1$ according to the level of requirement on Eve's decodability of confidential messages. Here, we simply select $\theta = 0.8$ as an example.

received SNR at Eve, the probability of error at Eve should decrease, and the secrecy performance should become worse. Therefore, we see that the secrecy performance of wireless transmissions cannot always be properly characterized by the existing perfect secrecy outage formulation. In contrast, the generalized secrecy outage probability ($\theta = 0.8$) increases with the improvement of Eve's channel condition, which properly captures the change of secrecy performance. By this specific example of the transmission with an ordinary code, we see that the generalized secrecy outage formulation is able to reveal some information about the secrecy performance of wireless transmissions that cannot be captured by the existing perfect secrecy outage formulation.

Figure 3 plots the average fractional equivocation which gives an asymptotic lower bound on Eve's decoding error probability. As shown in the figure, even when an ordinary code is used instead of the wiretap code, i.e., $R_b = R_s = 4$, Eve still suffers from a relatively high decoding error probability, e.g., $P_e > 0.78$ for $\bar{\gamma_e} = 1$. Figure 4 looks into the average information leakage rate of the transmissions. As the figure shows, the average information leakage rate, R_L, increases, as the confidential information rate, R_s, increases. However, R_L does not reach R_s even when R_s goes to $R_b = 4$.

V. Conclusions

To address the limitations of the existing secrecy outage formulation, in this paper, we proposed new secrecy measures for wireless transmissions where perfect secrecy is not always achievable. Compared with the existing secrecy outage probability, the newly proposed measures are wider applicable and provide more comprehensive understanding of the physical layer security performance over wireless fading channels. Specifically, the generalized secrecy outage probability is applicable for systems with different secrecy requirements on the decodability of messages at the eavesdropper. The asymptotic lower bound on eavesdropper's decoding error probability gives a worst-case estimation of eavesdropper's decodability. The average information leakage rate captures how fast the confidential information is leaked to the eavesdropper. Both analytical and numerical results show that the proposed secrecy measures can give insights on the secrecy performance of wireless transmissions that sometimes cannot be captured by the existing outage-based secrecy measure.

Besides, in this paper, we considered only the fixed-rate wiretap code as an example to illustrate the use of proposed secrecy measures in a given scenario. A possible future work is to evaluate the proposed secrecy measures with more transmission schemes.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[2] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[3] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, Sept. 2013.

[4] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[5] 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, June 2008.

[6] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[7] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sept. 2011.

[8] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, June 2012.

[9] N. Merhav, "Exact correct-decoding exponent of the wiretap channel decoder," 2014. [Online]. Available: http://arxiv.org/abs/1403.6143

[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[11] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley, 2006.

[13] M. Feder and N. Merhav, "Relations between entropy and error probability," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 259–266, Jan. 1994.

[14] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[15] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.