Rethinking the Secrecy Outage Formulation: A Secure Transmission Design Perspective

Xiangyun Zhou, *Member, IEEE*, Matthew R. McKay, *Member, IEEE*, Behrouz Maham, *Member, IEEE*, and Are Hjørungnes, *Senior Member, IEEE*

Abstract—This letter studies information-theoretic security without knowing the eavesdropper's channel fading state. We present an alternative secrecy outage formulation to measure the probability that message transmissions fail to achieve perfect secrecy. Using this formulation, we design two transmission schemes that satisfy the given security requirement while achieving good throughput performance.

Index Terms—Information-theoretic security, secrecy outage probability, channel state information.

I. INTRODUCTION

THE problem of achieving information-theoretic security over wireless channels without knowing the eavesdropper's instantaneous channel state information (CSI) has attracted considerable attention recently. The performance limits of such systems have been characterized in terms of the ergodic secrecy capacity (see, e.g., [1,2]), which captures the capacity limits under the constraint of perfect secrecy. This measure applies for delay-tolerant systems, assuming that the encoded messages span sufficient channel realizations to capture the ergodic features of the channel. For systems with stringent delay constraints, however, perfect secrecy cannot always be achieved, and outage-based characterizations become more appropriate by providing a probabilistic performance measure of secure communication.

The idea of secrecy outages has been adopted in [3,4], where an outage formulation was presented to capture the probability of having a transmission that is both reliable and secure [3–6]. As we will discuss, however, that formulation does not give a direct indication of the security level in the system, since it accounts for outage events which do not necessarily reflect failures in achieving perfect secrecy. In this letter, we put forth an alternative formulation which gives a more direct measure of system security, accounting for design parameters such as the rate of the transmitted codewords as well as the condition under which transmission is suspended. This new formulation provides a useful framework for computing the probability that transmitted messages are perfectly secure against eavesdropping. Based on our formulation, we also design two transmission schemes, each of which guarantees a certain level of security whilst maximizing the throughput. The first scheme requires CSI feedback from the legitimate receiver to the transmitter, whereas the second scheme requires only 1 bit of feedback.

II. SYSTEM MODEL

We consider the transmission of confidential messages from Alice to Bob over a Rayleigh fading channel in the presence of an eavesdropper, Eve. The transmit power, $\mathcal{P}$, is assumed fixed to the maximum level. The channel gains from Alice to Bob and Eve are denoted as h_b and h_e, both assumed to undergo independent quasi-static fading. The receiver noise variances at Bob and Eve are denoted by σ_b^2 and σ_e^2.

The instantaneous signal-to-noise ratios (SNRs) at Bob and Eve are given by $\gamma_b = \mathcal{P}|h_b|^2/\sigma_b^2$ and $\gamma_e = \mathcal{P}|h_e|^2/\sigma_e^2$, respectively, each having an exponential distribution given by

$$f_i(\gamma_i) = \frac{1}{\bar{\gamma}_i} \exp\left(-\frac{\gamma_i}{\bar{\gamma}_i}\right), \quad \gamma_i > 0, \quad i = b, e, \qquad (1)$$

where $\bar{\gamma}_b$ and $\bar{\gamma}_e$ are the average SNRs at Bob and Eve, respectively. We assume that Bob and Eve know their individual CSI perfectly and the statistics of both channels are known at Alice. We will consider different assumptions on the availability of Bob's instantaneous CSI at Alice, as discussed later. However, Eve's instantaneous CSI is unknown at Alice, and therefore perfect secrecy cannot always be achieved.

A. Existing Secrecy Outage Formulation

In the existing secrecy outage formulation [3,4], the outage event is defined as $\mathcal{O}(R_s) := \{C_s < R_s\}$, where $R_s > 0$ is the target secrecy rate, and[1]

$$C_s = [C_b - C_e]^+ = [\log_2(1 + \gamma_b) - \log_2(1 + \gamma_e)]^+ \qquad (2)$$

is the secrecy capacity, expressed in terms of Bob's channel capacity C_b and Eve's channel capacity C_e. The secrecy outage probability is defined as

$$p_{\text{out}} = \mathbb{P}(C_s < R_s). \qquad (3)$$

Here, an outage occurs whenever a message transmission is either unreliable (i.e., it cannot be decoded by Bob) or it is not perfectly secure (i.e., there is some information leakage to Eve). Whilst this secrecy outage formulation gives a fundamental characterization of the possibility of having a *reliable and secure* transmission, it does not distinguish between reliability and security. Hence, an outage does not necessarily imply a failure in achieving perfect secrecy. Furthermore, if Alice knows that Bob's channel cannot support the secrecy rate, i.e., $C_b < R_s$, then she would certainly suspend transmission. This "suspension event" falls within the outage event $\mathcal{O}(R_s)$, since $C_b < R_s$ implies $C_s < R_s$; however, it is clearly not a failure in achieving perfect secrecy. From a design perspective, it is important to provide an outage formulation which gives a more explicit measure of the level of security, in order to design transmission schemes which meet target security requirements.

---

[1]Here we employ the common notation, $[z]^+ = \max\{0, z\}$.

III. ALTERNATIVE SECRECY OUTAGE FORMULATION

We now present an alternative secrecy outage formulation which directly measures the probability that a *transmitted* message fails to achieve perfect secrecy. Consider the well-known Wyner's encoding scheme [7]: The encoder chooses two rates, namely, the rate of the transmitted codewords R_b, and the rate of the confidential information R_s. The rate difference $R_e \triangleq R_b - R_s$ reflects the cost of securing the message transmission against eavesdropping. For any transmitted message, Bob is able to decode correctly if $C_b > R_b$, whilst perfect secrecy fails if $C_e > R_e$. Hence, we define the secrecy outage probability as the conditional probability

$$p_{\text{so}} \triangleq \mathbb{P}(C_e > R_b - R_s \,|\, \text{message transmission}), \quad (4)$$

conditioned upon a message actually being transmitted. Unlike the existing secrecy outage formulation, our new formulation takes into account the system design parameters, such as the rate of the transmitted codewords *as well as* the condition under which message transmissions take place, and therefore provides a more explicit measure of the level of security. When transmission always occurs, which is usually the case if Alice has absolutely no knowledge about the instantaneous CSI of Bob's channel, the secrecy outage probability reduces to the unconditional probability $\mathbb{P}(C_e > R_b - R_s)$, which was considered in [8]. More generally, when some form of instantaneous CSI of Bob's channel is available, Alice can decide whether or not to transmit with possibly variable rates according to the channel condition. This is important since, as we will see, by carefully designing the condition for transmission, it is possible to dramatically reduce the secrecy outage probability. With this new formulation, the system designer can use the secrecy outage probability to characterize the security level and design transmission schemes that meet target security requirements.

IV. SECURE TRANSMISSION DESIGN

In this section, we consider the design problem of maximizing the throughput $\eta = p_{\text{tx}}R_s$, where p_{tx} denotes the probability of transmission. Note that p_{tx} can be interpreted as a quality of service (QoS) measure.[2] The primary design requirement is on the security level. In addition, one can impose another constraint on the probability of transmission as a QoS requirement. The design problem can be written as

$$\max \eta, \quad \text{s.t. } p_{\text{so}} \leq \epsilon, \ p_{\text{tx}} \geq \sigma, \quad (5)$$

where $\epsilon \in [0, 1]$ and $\sigma \in [0, 1]$ represent the minimum security and QoS requirements. The controllable design parameters are the rate of the transmitted codewords, R_b, the rate of the confidential information, R_s, as well as the condition for transmission. In the following, we consider the design of two different transmission schemes, based on Alice having either full or limited knowledge of the instantaneous CSI of Bob's channel. The condition for transmission is given by an on-off scheme; i.e., transmission takes place whenever the value of γ_b exceeds some SNR threshold μ. Note that $\mu \geq 2^{R_s} - 1$ always holds, since transmission can only happen when $C_b \geq R_s$.

A. Adaptive Encoder with On-Off Transmission

First, we consider the scenario where the encoder is able to adaptively choose the rate of the transmitted codewords, R_b, according to the instantaneous CSI of Bob's channel. In fact, only the instantaneous SNR, γ_b, needs to be fed back from Bob to Alice. The encoder sets R_b arbitrarily close to C_b, i.e., the largest possible rate without incurring any decoding error at Bob. For any given values of R_s and μ, we can compute the transmission probability as

$$p_{\text{tx}} = \mathbb{P}(\gamma_b > \mu) = \exp(-\mu/\bar{\gamma}_b). \quad (6)$$

Also, the secrecy outage probability is given by

$$
\begin{aligned}
p_{\text{so}} &= \mathbb{P}(C_e > C_b - R_s \,|\, \gamma_b > \mu) \\
&= \mathbb{P}\left(\gamma_b < 2^{R_s}(1 + \gamma_e) - 1 \,|\, \gamma_b > \mu\right) \\
&= \frac{\mathbb{P}\left(\mu < \gamma_b < 2^{R_s}(1 + \gamma_e) - 1\right)}{\mathbb{P}(\gamma_b > \mu)} \\
&= \exp\left(\frac{\mu}{\bar{\gamma}_b}\right) \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \left(\int_{\mu}^{2^{R_s}(1+\gamma_e)-1} f_b(\gamma_b) \mathrm{d}\gamma_b\right) f_e(\gamma_e)\mathrm{d}\gamma_e \\
&= \frac{\bar{\gamma}_e 2^{R_s}}{\bar{\gamma}_e 2^{R_s} + \bar{\gamma}_b} \exp\left(-\frac{\mu + 1 - 2^{R_s}}{\bar{\gamma}_e 2^{R_s}}\right). \quad (7)
\end{aligned}
$$

We see that the SNR threshold for on-off transmission, μ, presents a trade-off between the QoS and security. More specifically, a higher security level can be achieved by compromising the QoS, which is done by choosing a larger μ.

Now, we consider the design problem of finding the values of R_s and μ that maximize the throughput[3], given by

$$
\begin{aligned}
\arg\max_{R_s, \mu} \quad & p_{\text{tx}}(\mu)\, R_s, \\
\text{s.t.} \quad & p_{\text{so}}(\mu, R_s) \leq \epsilon, \ p_{\text{tx}}(\mu) \geq \sigma, \ \mu \geq 2^{R_s} - 1, \ R_s > 0,
\end{aligned}
$$

where we have explicitly shown the dependence of p_{tx} and p_{so} on μ and R_s. To solve this problem, we first establish an expression for the optimal μ for any given R_s as follows: Using (6), the feasible range of μ that satisfies $p_{\text{tx}}(\mu) \geq \sigma$ is found as $\mu \in [2^{R_s}-1, \bar{\gamma}_b \ln \sigma^{-1}]$. The throughput maximizing μ takes its smallest possible value while satisfying the security constraint. Since $p_{\text{so}}(\mu, R_s)$ in (7) is a decreasing function of μ, we obtain the optimal μ as

$$
\mu = \begin{cases} 2^{R_s}-1, & \text{if } R_s \leq \log_2 \frac{\bar{\gamma}_b \epsilon}{\bar{\gamma}_e(1-\epsilon)}, \\ 2^{R_s}(1 - \bar{\gamma}_e \ln \epsilon + \bar{\gamma}_e \ln \frac{\bar{\gamma}_e 2^{R_s}}{\bar{\gamma}_e 2^{R_s} + \bar{\gamma}_b})-1, & \text{otherwise}, \end{cases}
$$

where the first case presents the scenario that setting μ to its smallest value still satisfies the security constraint of $p_{\text{so}} \leq \epsilon$; otherwise, we have the second case by solving $p_{\text{so}} = \epsilon$.

The condition for having secure communication with some positive rate while satisfying both constraints can be found as

$$\epsilon > \frac{\bar{\gamma}_e}{\bar{\gamma}_e + \bar{\gamma}_b} \sigma^{\bar{\gamma}_b/\bar{\gamma}_e}.$$

Under this condition, we can formulate the optimization problem as

$$
\begin{aligned}
\arg\max_{R_s} \quad & R_s \exp(-\mu/\bar{\gamma}_b), \\
\text{s.t.} \quad & R_s > 0, \ \mu \leq \bar{\gamma}_b \ln \sigma^{-1},
\end{aligned}
$$

where μ is a function of R_s, whose expression was found above. Although the dependence of μ on R_s makes it difficult

---

[2]For strictly delay-limited systems, $1 - p_{\text{tx}}$ represents the probability of a message packet being dropped. For systems allowing moderate delays, $p_{\text{tx}}^{-1} - 1$ may give an indication of the average delay of transmission.

[3]Ideally, one can adaptively change R_s according to the instantaneous SNR. However, the optimal solution for this adaptive design is very difficult to obtain. Here, we look for the optimal R_s that is constant over time.
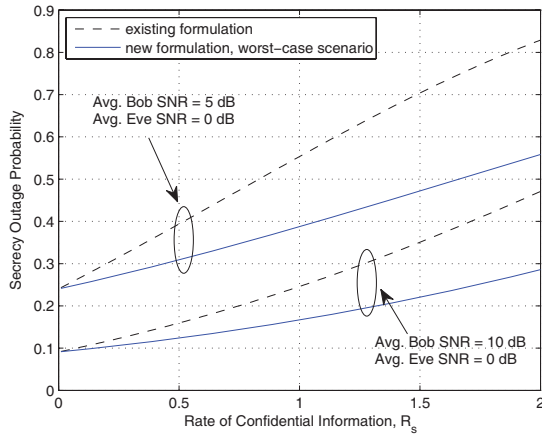
Fig. 1. Comparison between existing and new secrecy outage formulations.

Fig. 2. Throughput of secure transmission versus the security constraint. The QoS constraint is fixed to $\sigma = 0.5$.

to obtain a closed-form solution, this problem can be easily solved numerically.

B. Non-Adaptive Encoder with On-Off Transmission

Now we consider the transmission design with a non-adaptive encoder in which the rate of the codewords, R_b, is constant over time (but needs to be optimally chosen). In contrast to the adaptive encoder design which requires the feedback of the instantaneous SNR, this design only requires 1 bit of feedback to enable the on-off transmission scheme. For any given values of R_b, R_s, and μ, the transmission probability is given by (6) and the secrecy outage probability is given by

$$p_{\text{so}} = \mathbb{P}(C_e > R_b - R_s \mid \gamma_b > \mu) = \mathbb{P}(C_e > R_b - R_s)$$
$$= \exp\left(-\frac{2^{R_b - R_s} - 1}{\bar{\gamma}_e}\right). \qquad (8)$$

Again, we consider the design problem of finding the values of R_b, R_s and μ that maximize the throughput, given by

$$\arg\max_{R_b, R_s, \mu} \quad p_{\text{tx}}(\mu)\, R_s,$$
$$\text{s.t. } p_{\text{so}}(R_b, R_s) \le \epsilon,\ p_{\text{tx}}(\mu) \ge \sigma,\ \mu \ge 2^{R_b} - 1,\ R_s > 0.$$

We first establish expressions for the optimal μ and R_s for any given R_b as follows: Since $p_{\text{so}}(R_b, R_s)$ in (8) is independent of μ, it is optimal to minimize μ in order to maximize $p_{\text{tx}}(\mu)$ in (6). Hence, we obtain the optimal μ as

$$\mu = 2^{R_b} - 1.$$

Note that $R_b \le \log_2(1 + \bar{\gamma}_b \ln \sigma^{-1})$ is required or $p_{\text{tx}}(\mu) \ge \sigma$ can never be satisfied. For any given R_b, the throughput maximizing R_s takes its maximum possible value while satisfying $p_{\text{so}}(R_b, R_s) \le \epsilon$. Hence, we obtain the optimal R_s as

$$R_s = R_b - \kappa, \quad \text{where } \kappa = \log_2(1 + \bar{\gamma}_e \ln \epsilon^{-1}).$$

The condition for having secure communication with some positive rate while satisfying both constraints can be found as

$$\epsilon > \sigma^{\bar{\gamma}_b / \bar{\gamma}_e}.$$

Under this condition, we can formulate the optimization problem as

$$\arg\max_{R_b} \quad (R_b - \kappa) \exp\left(-\frac{2^{R_b} - 1}{\bar{\gamma}_b}\right),$$
$$\text{s.t. } \kappa < R_b \le \log_2(1 + \bar{\gamma}_b \ln \sigma^{-1}),$$

which in this case admits the explicit solution

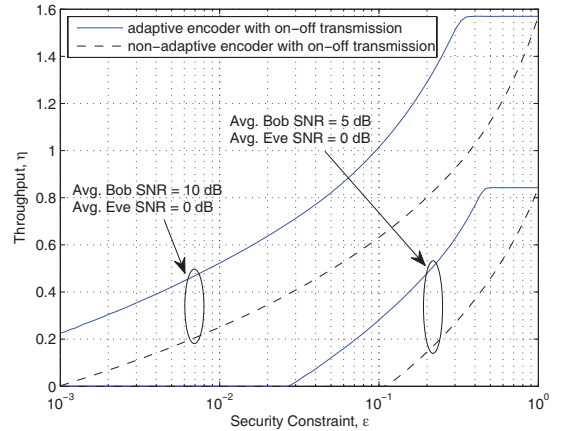$$R_b = \min\left\{\kappa + \frac{1}{\ln 2} W_0\left(\bar{\gamma}_b \exp(-\kappa \ln 2)\right),\ \log_2(1 + \bar{\gamma}_b \ln \sigma^{-1})\right\},$$

where $W_0(\cdot)$ is the principal branch of Lambert's W function.

V. NUMERICAL RESULTS AND DISCUSSION

Fig. 1 presents the secrecy outage probability, comparing the existing formulation (3) and the new formulation (7). In both cases, the rate of transmitted codewords is adaptively chosen as $R_b = C_b$. For the new formulation, the on-off SNR threshold is set to its minimum value of $\mu = 2^{R_s} - 1$, which gives the maximum outage probability. We see from the figure that the outage probabilities predicted by the two formulations differ significantly. Hence, the existing formulation cannot be directly used to measure the security level.

Fig. 2 compares the achievable throughput of our proposed adaptive and non-adaptive encoder designs, for a range of security constraints. The QoS constraint is fixed to $\sigma = 0.5$. We see that it is generally impossible to achieve arbitrarily low secrecy outage probability, which agrees with the lower bounds on the secrecy outage probability derived in Section IV. This figure also shows that a significant throughput improvement is obtained by adaptively changing the rate of the transmitted codewords based on knowledge of Bob's instantaneous CSI. On the other hand, the design with non-adaptive encoder only requires 1 bit of feedback, which minimizes the feedback overhead.

REFERENCES

[1] 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.

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: the MISOME channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[3] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inform. Theory*, Sep. 2005, pp. 2152–2155.

[4] 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.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[6] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–6.

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

[8] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.