A Versatile Secure Transmission Strategy in the Presence of Outdated CSI

Jianwei Hu, *Student Member, IEEE,* Nan Yang, *Member, IEEE,* Xiangyun Zhou, *Member, IEEE,* Weiwei Yang, *Member, IEEE,* and Yueming Cai, *Senior Member, IEEE*

***Abstract*—We study secure transmission considering the practical scenario where only outdated knowledge of the legitimate receiver's channel and statistical knowledge of the eavesdropper's channel is available at the transmitter. Conditioned on the limited channel knowledge, we adopt an on-off secure transmission scheme and propose a versatile strategy to determine the codeword transmission rate. We first analyze the outage performance of the system and then provide the design of optimal wiretap code parameters maximizing the secrecy throughput. Compared with the existing solution in the literature, the proposed secure transmission design enlarges the achievable reliability-security region and increases the maximum secrecy throughput.**

***Index Terms*—Physical layer security, outdated CSI, reliability-security region, secrecy throughput.**

I. Introduction

The security of information transmission is becoming an increasingly important concern in many wireless applications, such as online banking and transmission of private medical data [1]. As a promising method to enhance security, *physical layer security* has recently attracted considerable attention. An important assumption in previous studies is the availability of perfect channel knowledge of the receivers at the transmitter. However, it is practically impossible for the transmitter to know the eavesdropper's channel state information (CSI) if the eavesdropper is a passive device. Even the assumption of the transmitter perfectly knowing the legitimate receiver's CSI is very idealistic. Therefore, recent studies have focused on the realistic scenarios with imperfect CSI at the transmitter. Specifically, an on-off scheme was designed in [2] to improve the secrecy performance when the estimated CSI at the receivers is not perfect. In [3], an artificial-noise-aided beamforming scheme was optimized to guarantee a satisfactory level of secrecy when the CSI feedback link is rate-constrained. Meanwhile, some research efforts have been devoted towards the outdated CSI caused by the feedback delay [4, 5]. We note that [4, 5] merely concentrated on the performance analysis without further looking into the optimal design of practical secure transmission schemes.

In this work, we consider a single-antenna system, i.e., a single-input single-output single-eavesdropper (SISOSE) scenario. Considering only outdated knowledge of the legitimate receiver's channel and statistical knowledge of the eavesdropper's channel available at the transmitter, we design a new secure transmission scheme based on the celebrated Wyner's wiretap code. The key challenges faced in this specific scenario are the existence of two different outage events. The first outage event, referred to as *connection outage event*, results from the imperfect channel knowledge of the desired communication channel. The second outage event, referred to as *secrecy outage event*, is caused by the fact that the eavesdropper remains quiet and its instantaneous CSI is unavailable to the transmitter. In order to guarantee the target levels of reliability and security, one should keep the two outage events under control when designing any secure transmission scheme. Then the resulting design problem becomes: *Given connection and secrecy outage constraints, how to determine wiretap code parameters with the aforementioned practical CSI assumption?*

To overcome this problem, in this work we design a new and versatile strategy to determine the optimal codeword transmission rate achieving the maximum secrecy throughput. We highlight that this strategy makes a significant advancement than our latest contribution in [6]. In [6], the transmission scheme for perfect CSI of the legitimate channel was directly applied for the imperfect CSI case, such that the codeword transmission rate is chosen as the estimated main channel capacity. Different from [6], in this work we choose the codeword transmission rate as a function of the estimated main channel capacity, the secrecy rate, and a flexible tradeoff coefficient. Using this function, our design achieves a larger feasible reliability-security region and thus a higher maximum secrecy throughput. Centering on this versatile design, we first derive an easy-to-compute expression for the secrecy throughput. Based on this expression, we determine the optimal wiretap code parameters that maximize the secrecy throughput. Importantly, we find that the optimal codeword transmission rate is smaller than the estimated main channel capacity, which explains the advantage of our design over that in [6]. The performance analysis and design guidelines presented in this paper offer pivotal insights into the effective management of the outdated CSI for achieving the desired levels of reliability and security.

II. System Model

We consider a wiretap channel where the communication between the legitimate transmitter, Alice, and the legitimate receiver, Bob, is overheard by an eavesdropper, Eve. We assume that Alice, Bob, and Eve are equipped with a single antenna each. The Alice-Bob channel and the Alice-Eve channel are referred to as the main channel and the eavesdropper's channel, respectively. We also assume that the main channel coefficient and the eavesdropper's channel coefficient are independent and identically distributed (i.i.d.) zero-mean circularly symmetric complex Gaussian random variables with unit variance across the coherence blocks. We focus on the practical passive eavesdropping scenario where the instantaneous CSI of the eavesdropper's channel is not known at Alice. This scenario can also be seen as a robust scenario for secrecy which allows for Eve's malicious behaviors, e.g., deliberately feeding back false CSI [2].

In this work, we assume that the instantaneous CSI of the main channel obtained at Alice is outdated. In practice, the process of acquiring CSI at Alice may take a long time duration for pilot training, channel estimation, and CSI feedback. It follows that the main channel knowledge received at Alice may be outdated for the subsequent data transmission. Under this assumption, we denote $h_b \sim \mathcal{CN}(0,1)$ as the main channel coefficient obtained during the channel estimation and feedback process. We also denote $\hat{h}_b \sim \mathcal{CN}(0,1)$ as the main channel coefficient in data transmission process. As such, $\hat{h}_b$ is the τ_d time-delayed version of h_b, as characterized by the Gauss-Markov model [7–9]. Mathematically, $\hat{h}_b$ is expressed as

$$\hat{h}_b = \rho h_b + \sqrt{1-\rho^2} w_b, \tag{1}$$

This work of J. Hu, W. Yang, and Y. Cai was supported by the National Natural Science Foundation of China (No. 61371122, No. 61471393 and No. 61501512). The work of N. Yang and X. Zhou was supported by the Australian Research Council Discovery Project (DP150103905).

J. Hu, W. Yang, and Y. Cai are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail: hujianwei1990@yeah.net, wwyang1981@163.com, caiym@vip.sina.com).

N. Yang and X. Zhou are with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (email: {nan.yang, xiangyun.zhou}@anu.edu.au).

Digital Object Identifier 10.1109/TVT.2016.2550032

where ρ is the correlation coefficient between $\hat{h}_b$ and h_b, and $w_b \sim \mathcal{CN}(0,1)$ is the channel-independent error in the main channel. As per the Clark's fading model, ρ is formulated as $\rho = J_0(2\pi f_d \tau_d)$, where $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind and f_d is the maximum Doppler frequency at the receiver.

Based on (1), the received signal at Bob during the data transmission process is given by

$$y_b = \sqrt{P} d_b^{-\frac{\mu}{2}} \hat{h}_b x + n_b, \tag{2}$$

where P denotes the transmit power, d_b and μ denote the distance and the path loss exponent (PLE) between Alice and Bob, respectively, x denotes the transmit signal, and $n_b \sim \mathcal{CN}\left(0, \sigma_b^2\right)$ denotes the additive white Gaussian noise (AWGN) at Bob. Accordingly, the instantaneous received signal-to-noise ratios (SNR) at Bob during the data transmission process is given by $\hat{\gamma}_b = |\hat{h}_b|^2 P d_b^{-\mu}/\sigma_b^2$. It is worth mentioning that the knowledge obtained at Alice based on the feedback from Bob is $\gamma_b = |h_b|^2 P d_b^{-\mu}/\sigma_b^2$, but not $\hat{\gamma}_b$.

We now present the preliminary statistical results of $\hat{\gamma}_b$ and γ_b to facilitate our performance analysis. We note that both $\hat{\gamma}_b$ and γ_b have an exponential distribution. Hence, the probability density functions (PDFs) of $\hat{\gamma}_b$ and γ_b are uniformly expressed as

$$f_{\Upsilon_b}(x) = \frac{1}{\overline{\gamma}_b} e^{-\frac{x}{\overline{\gamma}_b}}, \tag{3}$$

where $\Upsilon_b \in \{\gamma_b, \hat{\gamma}_b\}$ and $\overline{\gamma}_b = P d_b^{-\mu}/\sigma_b^2$ denotes the average received SNR at Bob. We also note that $\hat{\gamma}_b$ and γ_b are correlated random variables. As a result, the conditional PDF of $\hat{\gamma}_b$ conditioned on a given γ_b is given by [10]

$$f_{\hat{\gamma}_b|\gamma_b}(y\,|x) = \frac{1}{(1-\rho^2)\overline{\gamma}_b} e^{-\frac{y+\rho^2 x}{(1-\rho^2)\overline{\gamma}_b}} I_0\left(\frac{2\rho\sqrt{xy}}{(1-\rho^2)\overline{\gamma}_b}\right). \tag{4}$$

We next formulate the eavesdropper's channel. The received signal at Eve during the data transmission process is given by

$$y_e = \sqrt{P} d_e^{-\frac{\nu}{2}} \hat{h}_e x + n_e, \tag{5}$$

where $\hat{h}_e \sim \mathcal{CN}(0,1)$ denotes the eavesdropper's coefficient during data transmission process, d_e and ν denote the distance and the PLE between Alice and Eve, respectively, and $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ denotes the AWGN at Eve. The instantaneous received SNR at Eve during the data transmission process is accordingly written as $\hat{\gamma}_e = |\hat{h}_e|^2 P d_e^{-\nu}/\sigma_e^2$. Note that $\hat{\gamma}_e$ has an exponential distribution. As such, its PDF is given by

$$f_{\hat{\gamma}_e}(x) = \frac{1}{\overline{\gamma}_e} e^{-\frac{x}{\overline{\gamma}_e}}, \tag{6}$$

where $\overline{\gamma}_e = P d_e^{-\nu}/\sigma_e^2$ denotes the average received SNR at Eve. Although we assume that the instantaneous CSI of the eavesdropper's channel is not known at Alice, we assume that the statistical CSI, $\overline{\gamma}_e$, is known at Alice [5, 10, 11].

In the wiretap channel Alice determines the wiretap code parameters in order to achieve the secrecy rate of R_s. Specifically, Alice constructs a parameter pair (R_b, R_e) for the wiretap code [12], where R_b denotes the transmission rate of the codeword, R_e denotes the rate redundancy which provides secrecy against eavesdropping, and $R_s = R_b - R_e$. We note that the only knowledge about the main channel obtained at Alice is the main channel capacity[1] given by $C_b = \log_2(1+\gamma_b)$. As such, Alice needs to design the wiretap code parameters based on C_b solely. Our proposed new design of the wiretap code parameters and the corresponding secure transmission schemes will be detailed in Section III.

[1]We clarify that Alice cannot obtain the main channel capacity and the eavesdropper's channel capacity during the data transmission process, given by $\hat{C}_b = \log_2(1+\hat{\gamma}_b)$ and $\hat{C}_e = \log_2(1+\hat{\gamma}_e)$, respectively.

III. New Design of Secure Transmission

In this section, we first formulate the principle of our new design of the wiretap code parameters. Using this design, we then analyze the secrecy performance of the on-off transmission scheme and evaluate the feasibility of the reliability and security constraints. Finally, we solve the optimization problems of the secrecy throughput subject to outage constraints.

A. Design of Wiretap Code Parameters

In this work we propose a new *versatile* design to determine the optimal wiretap code parameters, which achieves a flexible tradeoff between reliability and security. The versatility of our design lies in the introduction of a tradeoff coefficient u, where $u \in (0,1]$. Mathematically, our design is expressed as

$$R_b = \log_2\left(2^{R_s} + u\left(2^{C_b} - 2^{R_s}\right)\right), \tag{7}$$

which indicates that R_b is determined by R_s, u, and C_b. Based on (7) and the range of u, we find that the value of R_b is within the feasible range of $(R_s, C_b]$. Compared with the design of $R_b = C_b$ in [6], this design enables versatility on the choice of R_b for distinct transmission blocks.

We highlight that in our design, R_b is adaptively determined according to the feedback from Bob, while R_s is optimally chosen and kept constant over the whole transmission period. This indicates that our design can be treated as a semi-adaptive-R_b but fixed-R_s scheme. Compared with the fully-adaptive strategies in the literature, e.g., those from [13–16], we clarify that our semi-adaptive strategy serves as a practically valuable enabler to provide the closed-form expressions for the connection outage probability and secrecy outage probability. As such, it facilitates us to design wiretap code parameters under dual outage constraints in real time, without resorting to complicated optimization-oriented signal processing algorithms. Of course, this advantage is achieved at the cost of not achieving the optimal performance.

B. Secrecy Performance Analysis

The on-off transmission scheme, which allows Alice to transmit only when the main channel quality meets some predetermined requirements, has attracted considerable attention in recent physical layer security studies due to its ease of implementation [2, 3, 17, 18]. In our work, we apply this scheme since γ_b is the only channel knowledge obtained by Alice. Under this scheme, Alice transmits only when $C_b \geq R_s$. We next present detailed analysis of the governing secrecy performance metrics for the on-off transmission scheme.

1) Transmission Probability: The transmission probability is formulated as

$$p_{tx}(R_s) = \Pr\{C_b \geq R_s\}. \tag{8}$$

Using the cumulative density distribution (CDF) of γ_b, we obtain $p_{tx}(R_s)$ as

$$p_{tx}(R_s) = \Pr\left\{\gamma_b \geq 2^{R_s} - 1\right\} = e^{-\frac{2^{R_s}-1}{\overline{\gamma}_b}}. \tag{9}$$

2) Connection Outage Probability: The connection outage occurs when the instantaneous main channel quality during the data transmission process cannot support R_b, i.e., $\hat{C}_b < R_b$. Accordingly, the connection outage probability is given by

$$p_{co}(u, R_s) = \Pr\left\{\hat{C}_b < R_b \,|\text{transmission}\right\}. \tag{10}$$

We clarify that the connection outage probability defined in (10) is the probability of the connection outage event conditioned on the

transmission event. That is, transmission outage is excluded from the characterization of the connection outage probability. Using (8) and (10), we derive the connection outage probability as

$$\begin{aligned} p_{co}\left(u,R_s\right) &= \Pr\left\{\hat{C}_b < R_b \,|C_b \geq R_s\right\} \\ &= 1 - e^{\frac{\left(u-\rho^2\right)\left(2^{R_s}-1\right)}{\left(1-\rho^2\right)\overline{\gamma}_b}} \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\left(1-\rho^2\right)\rho^{2(n+k)}}{\Gamma\left(n+k+1\right)k!} \\ &\quad \times \sum_{q=0}^{k}\binom{k}{q}\frac{(1-u)^{k-q}\left(2^{R_s}-1\right)^{k-q}u^q}{\left(\left(1-\rho^2\right)\overline{\gamma}_b\right)^{k-q}(1+u)^{n+k+q+1}} \\ &\quad \times \Gamma\left(n+k+q+1, \frac{(1+u)\left(2^{R_s}-1\right)}{\left(1-\rho^2\right)\overline{\gamma}_b}\right), \end{aligned} \tag{11}$$

where $\Gamma\left(\cdot\right)$ and $\Gamma\left(\cdot,\cdot\right)$ are the Gamma function and the incomplete Gamma function defined in [19]. We claim that the proof of (11) is similar to the derivation for [6, Eq. (12)]. Hence, in this work we omit detailed proof.

3) Secrecy Outage Probability: The secrecy outage occurs when the rate redundancy R_e is lower than the instantaneous eavesdropper's channel capacity during the data transmission process, i.e., $R_e < \hat{C}_e$. Mathematically, the secrecy outage probability is given by

$$p_{so}\left(u,R_s\right) = \Pr\left\{R_e < \hat{C}_e \,|\text{transmission}\right\}. \tag{12}$$

Using (8) and (12), we derive the connection outage probability as

$$p_{so}\left(u,R_s\right) = \Pr\left\{R_e < \hat{C}_e \,|C_b \geq R_s\right\} = \frac{2^{R_s}\overline{\gamma}_e}{2^{R_s}\overline{\gamma}_e + u\overline{\gamma}_b}. \tag{13}$$

4) Reliable-and-Secure Connection Probability: To examine the reliability and security in a unified manner, we define the reliable-and-secure connection probability[2] as

$$p_{r\&s}\left(u,R_s\right) = \Pr\left\{\hat{C}_b \geq R_b, R_e \geq \hat{C}_e \,|\text{transmission}\right\}. \tag{14}$$

Using (8) together with (14), we derive the reliable-and-secure connection probability as

$$\begin{aligned} p_{r\&s}\left(u,R_s\right) &= \Pr\left\{\hat{C}_b \geq R_b, R_e \geq \hat{C}_e \,|C_b \geq R_s\right\} \\ &= e^{\frac{2^{R_s}-1}{\overline{\gamma}_b}}\left(\ell_1 - \ell_2\right), \end{aligned} \tag{15}$$

where ℓ_1 is given by

$$\begin{aligned} \ell_1 = &\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\rho^{2(n+k)}\left(1-\rho^2\right)}{2^{n+2k+1}\Gamma\left(k+1\right)\Gamma\left(n+k+1\right)} \\ &\times \Gamma\left(n+2k+1, \frac{2\left(2^{R_s}-1\right)}{\left(1-\rho^2\right)\overline{\gamma}_b}\right), \end{aligned} \tag{16}$$

and ℓ_2 is given by

$$\begin{aligned} \ell_2 = &e^{-\frac{(1-u)2^{R_s}\overline{\gamma}_e - u\left(1-\rho^2\right)\overline{\gamma}_b}{\left(1-\rho^2\right)2^{R_s}\left(2^{R_s}-1\right)^{-1}\overline{\gamma}_b\overline{\gamma}_e}} \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\rho^{2(n+k)}\left(1-\rho^2\right)}{k!\Gamma\left(n+k+1\right)} \\ &\times \sum_{q=0}^{k}\binom{k}{q}\frac{(1-u)^{k-q}\left(2^{R_s}-1\right)^{k-q}u^q}{\left(\left(1-\rho^2\right)\overline{\gamma}_b\right)^{k-q}} \\ &\times \Gamma\left(n+k+q+1, \frac{\left(u\left(1-\rho^2\right)\overline{\gamma}_b + (1+u)\,2^{R_s}\overline{\gamma}_e\right)}{\left(2^{R_s}-1\right)^{-1}\left(1-\rho^2\right)2^{R_s}\overline{\gamma}_b\overline{\gamma}_e}\right) \\ &\times \left(\frac{2^{R_s}\overline{\gamma}_e}{u\left(1-\rho^2\right)\overline{\gamma}_b + (1+u)\,2^{R_s}\overline{\gamma}_e}\right)^{n+k+q+1}. \end{aligned} \tag{17}$$

[2]We note that the connection outage and the secure outage are not mutually exclusive, indicating that the reliable-and-secure connection probability between Alice and Bob is not equal to $1 - p_{co} - p_{so}$.

C. Feasibility of Outage Constraints

To guarantee the reliability and security levels of the wiretap channel, we practically introduce a reliability constraint ϵ and a security constraint δ in the design. Since the channel knowledge known at Alice is limited, we next examine the feasible ranges of ϵ and δ for a given u.

Using (11), we numerically find that $p_{co}\left(u,R_s\right)$ is an increasing function of R_s for a given u. When $R_s = 0$, $p_{co}\left(u,R_s\right)$ achieves its lower bound, $p_{co,LB}\left(u\right)$, which is derived as

$$p_{co,LB}\left(u\right) = 1 - \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{(n+2k)!\rho^{2(n+k)}\left(1-\rho^2\right)u^k}{k!\,(n+k)!\,(1+u)^{n+2k+1}}. \tag{18}$$

Accordingly, the feasible range of ϵ is obtained as

$$p_{co,LB}\left(u\right) < \epsilon \leq 1. \tag{19}$$

We next observe (13) and find that $p_{so}\left(u,R_s\right)$ is also an increasing function of R_s for a given u. Thus, $p_{so}\left(u,R_s\right)$ achieves its lower bound, $p_{so,LB}\left(u\right)$, when $R_s = 0$. This bound is derived as

$$p_{so,LB}\left(u\right) = \frac{\overline{\gamma}_e}{\overline{\gamma}_e + u\overline{\gamma}_b}. \tag{20}$$

The feasible range of δ is accordingly obtained as

$$p_{so,LB}\left(u\right) < \delta \leq 1. \tag{21}$$

Based on (19) and (21), we clarify that the versatility of u enables a tradeoff between reliability and security, leading to a larger feasible reliability-security region.

D. Optimization of Wiretap Code Parameters

In this subsection, we first define the primary performance indicator through this paper, i.e., the secrecy throughput. We then show that our versatile design achieves a higher maximum secrecy throughput. Finally, we present how to determine the optimal code parameters for maximizing the secrecy throughput subject to outage constraints.

1) Secrecy Throughput: Through this paper we adopt the secrecy throughput η as the preferred secrecy performance metric. Specifically, we define η as the product of the transmission probability p_{tx}, the reliable-and-secure connection probability $p_{r\&s}$, and the secrecy rate R_s. Mathematically, η is formulated as

$$\eta\left(u,R_s\right) = p_{tx}(R_s)p_{r\&s}\left(u,R_s\right)R_s, \tag{22}$$

where $p_{tx}(R_s)$ and $p_{r\&s}\left(u,R_s\right)$ are given by (8) and (14), respectively. We clarify that the incorporation of $p_{r\&s}$ allows us to measure the average rate of the confidential information reliably transmitted from Alice to Bob without being eavesdropped on by Eve.

2) The Benefit on the Maximum Secrecy Throughput: Considering no outage constraints, we find that for a given R_s, the optimal u maximizing $\eta(u,R_s)$ is the one that maximizes $p_{r\&s}(u,R_s)$. For a given R_s, we numerically find that $p_{r\&s}(u,R_s)$ first increases and then decreases as u increases from 0 to 1. This indicates that the optimal u maximizing $p_{r\&s}(u,R_s)$ is less than 1. Recall that [6] is merely a special case of this work with $u = 1$. Therefore, our versatile design leads to a higher maximum secrecy throughput. This emphasizes the potential advantage of the versatile design in terms of the secrecy throughput.

3) Optimization subject to Outage Constraints: We now determine the values of u and R_s that maximize the secrecy throughput subject to the connection and secrecy outage constraints. Given the fact that perfect connection and perfect secrecy cannot be guaranteed, such maximization is of practical importance since it keeps the

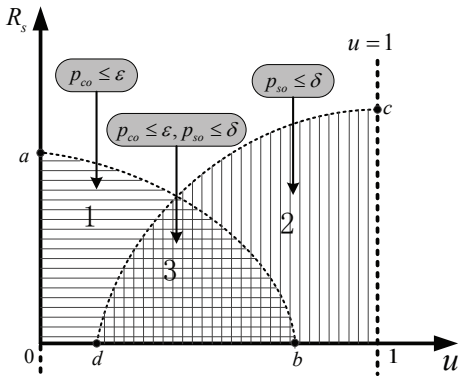

Fig. 1. Feasible region for u and R_s subject to connection and secrecy outage constraints.

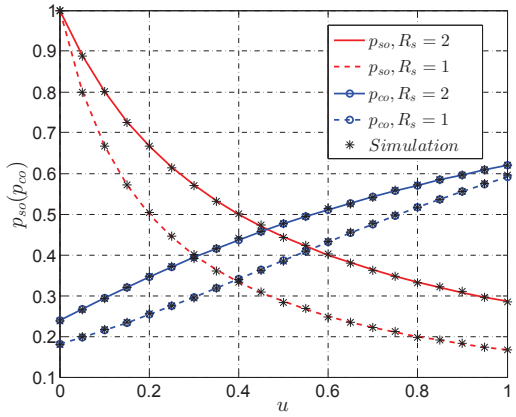

Fig. 2. Connection and secrecy outage probabilities versus u for $\rho = 0.5$, $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

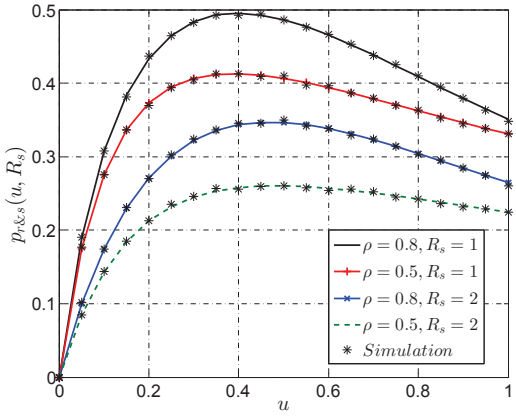

Fig. 3. Reliable-and-secure connection probability versus u for $\overline{\gamma}_b = 10$ dB, and $\overline{\gamma}_e = 0$ dB.

risk of decoding errors and being eavesdropped under control. The optimization problem is expressed as

$$\max_{u,R_s} \quad \eta\left(u, R_s\right), \\ \text{subject to} \quad p_{co} \le \epsilon, p_{so} \le \delta. \tag{23}$$

The feasibility of ϵ and δ are indicated by (19) and (21), respectively. Since ϵ and δ restrict the feasible region of the optimization problem in (23), we firstly need to examine the feasible region for u and R_s.

Based on (11) and (13), we conclude that a lower R_s for a fixed u leads to a lower p_{co} and a lower p_{so}, while a lower u for a fixed R_s leads to a lower p_{co} but a higher p_{so}. Thus we can use Fig. 1 to describe the sketch of the feasible region. Specifically, the shaded area 1 denotes the feasible region under the condition of $p_{co} \le \epsilon$, while the shaded area 2 denotes the feasible region under the condition of $p_{so} \le \delta$. As such, the overlap area 3 describes the feasible region of the optimization problem in (23). Therefore, we solve this optimization problem in two steps as follows:

Step 1: Determine the boundary lines, e.g., Arc-ab and Arc-cd. Assisted by (11), we express a and b as

$$a = \left\{R_s \left| p_{co}\left(0, R_s\right) = \epsilon\right.\right\}, \quad b = \left\{u \left| p_{co}\left(u, 0\right) = \epsilon\right.\right\}. \tag{24}$$

Although the closed-form solutions for a and b are mathematically intractable, we are able to obtain them using numerical search methods. Then the boundary line *Arc-ab* can be numerically found.

Assisted by (13), we express c and d as

$$c = \left\{R_s \left| p_{so}\left(1, R_s\right) = \delta\right.\right\} = \log_2\left(\frac{\delta\overline{\gamma}_b}{\left(1-\delta\right)\overline{\gamma}_e}\right), \tag{25}$$

and

$$d = \left\{u \left| p_{so}\left(u, 0\right) = \delta\right.\right\} = \frac{\left(1-\delta\right)\overline{\gamma}_e}{\delta\overline{\gamma}_b}, \tag{26}$$

respectively. Then the boundary line *Arc-cd* is determined.

Step 2: Search the optimum solutions, (u^*, R_s^*). After determining the boundary lines, the feasible region of u and R_s is identified. The final step is to find the optimal solutions maximizing the secrecy throughput by using numerical search methods, e.g., the grid-search method.

IV. Numerical Results

We present numerical results in this section to illustrate the benefits of our proposed *versatile* design. Throughout this section the simulation settings are as follows, unless specified otherwise: The average received SNR at Bob and Eve are assumed to be $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB, respectively.[3]

Fig. 2 plots the connection and secrecy outage probabilities for different values of R_s. In this figure, the theoretical curves for $p_{co}\left(u, R_s\right)$ and $p_{so}\left(u, R_s\right)$ are generated from (11) and (13), respectively. Importantly, we find that the Monte Carlo simulation points, marked by "$*$", match precisely with the analytical curves. This demonstrates the accuracy of our analysis. We first observe that for a fixed R_s, increasing u leads to a higher connection outage probability but a lower secrecy outage probability. This observation can be explained by the fact that when R_s is fixed, a higher u brings about a higher R_b, leading to a higher probability that $\tilde{C}_b$ is lower than R_b, but a lower probability that $\tilde{C}_e$ is larger than R_e. Second, we observe that for a fixed u, both $p_{co}\left(u, R_s\right)$ and $p_{so}\left(u, R_s\right)$ increases with the increase of R_s. This figure highlights that the versatility of u, which lies in its ability of enabling a tradeoff between the reliability and security.

Fig. 3 and Fig. 4 plot the reliable-and-secure connection probability versus u and R_s, respectively. In these figures, the theoretical curves for $p_{r\&s}\left(u, R_s\right)$ are generated from (15). Numerical simulations

[3]To evidently show the secrecy performance, numerical results for the case, where $\overline{\gamma}_b$ is comparable or lower than $\overline{\gamma}_e$, are not presented. We assume that Alice can use an external jammer to guarantee the advantage of the main channel's quality over the eavesdropper's channel's quality. However, this is beyond the scope of this work.

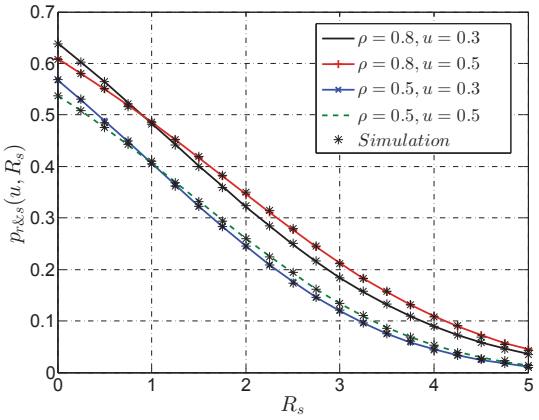

Fig. 4. Reliable-and-secure connection probability versus R_s for $\overline{\gamma}_b = 10$ dB, and $\overline{\gamma}_e = 0$ dB.

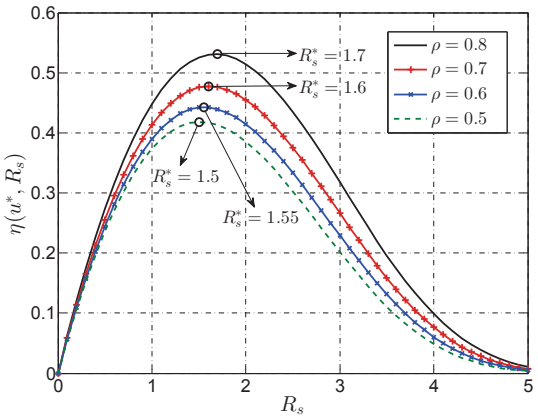

Fig. 6. Secrecy throughput versus R_s without dual outage constraints for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

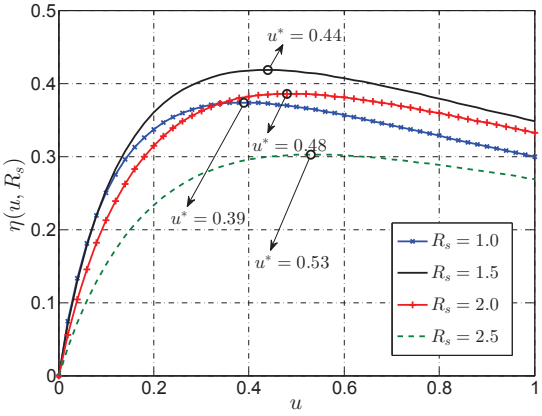

Fig. 5. Secrecy throughput versus u without dual outage constraints for $\rho = 0.5$, $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

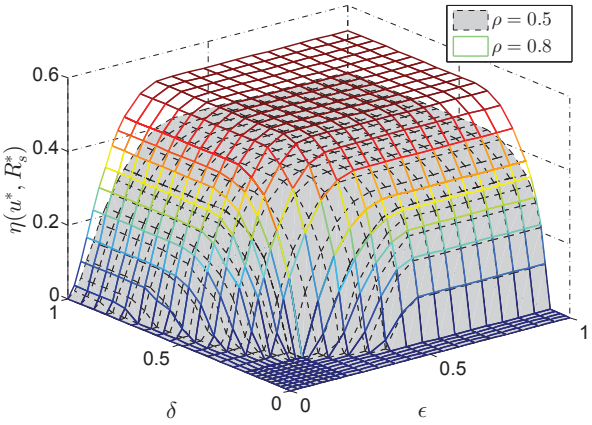

Fig. 7. Secrecy throughput subject to dual outage constraints for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

are presented to corroborate our analytical results. From Fig. 3, we observe that for a fixed R_s, $p_{r\&s}(u, R_s)$ first increases and then decreases with u. From Fig. 4, we observe that for a fixed u, $p_{r\&s}(u, R_s)$ decreases when R_s increases. Moreover, both Fig. 3 and Fig. 4 illustrate that $p_{r\&s}(u, R_s)$ decreases as ρ decreases. This is due to the fact that the uncertainty in the main channel increases as ρ decreases, which results in poorer reliability and security levels. Therefore, Fig. 3 and Fig. 4 highlight the enhancement in the reliability and security levels brought by the reduction in R_s and the optimization on u.

Fig. 5 plots the secrecy throughput versus u with $\rho = 0.5$ for different values of R_s. In this figure, the reliability and security constraints are not considered. We first observe that for a fixed R_s, $\eta(u, R_s)$ first increases and then decreases as u increases from 0 to 1, which confirms that an optimal u indeed exists such that the secrecy throughput is maximized for a fixed R_s. Second, we observe that u^* shifts to the right when R_s increases. For example, we find that when R_s increases from 1 to 1.5, u^* grows from 0.39 to 0.44. Third, we observe that it is not always beneficial to increase R_s. For example, when $\rho = 0.5$ we find that $R_s = 1.5$ achieves a higher secrecy throughput than $R_s = 2.0$ and $R_s = 2.5$. This observation indicates that there exists an optimal R_s maximizing the secrecy throughput.

Fig. 6 plots the secrecy throughput versus R_s with optimal u for different values of ρ. In this figure, the reliability and security constraints are not considered. We clarify that the value of u for each curve is optimized in this figure. We first observe that $\eta(u^*, R_s)$ first increases and then decreases when R_s increases, confirming the uniqueness of R_s^* maximizing $\eta(u^*, R_s)$ in Section III-D. Second, we observe that R_s^* shifts to the right when ρ increases. For example, we find that when ρ increases from 0.5 to 0.6, R_s^* grows from 1.5 to 1.55. Third, we observe that $\eta(u^*, R_s)$ increases when ρ becomes higher. This observation implies that a higher secrecy throughput is supported when more knowledge about the main channel is available at Alice.

Fig. 7 plots the secrecy throughput versus the reliability and security constraints for $\rho = 0.5$ and $\rho = 0.8$. In this figure, the curved surface for $\eta(u^*, R_s^*)$ subject to dual outage constraints is generated from (23). We first observe that a positive secrecy throughput only exists within the feasible region of the security and reliability constraints. We also observe that for a fixed δ (or ϵ), the secrecy throughput initially increases with ϵ (or δ) and then becomes saturated after ϵ (or δ) exceeds a certain threshold. For example, when $\rho = 0.8$, the thresholds for dual outage constraints are $\epsilon_{th} = 0.34$ and $\delta_{th} = 0.42$. We further observe that the maximum secrecy throughput is always achieved when the dual outage constraints exceed these thresholds. This is due to the fact that when the constraints are higher than ϵ_{th} and δ_{th}, the optimal u and R_s obtained without outage constraints can always be adopted to perform secure transmission.

V. Conclusion

In this work, we considered the SISOSE wiretap channel where only outdated knowledge of the main channel and statistical knowledge of the eavesdropper's channel are available at the transmitter. We designed a versatile strategy to choose the optimal codeword transmission rate for the on-off transmission scheme. Based on the performance analysis, we showed that how to determine the optimal wiretap code parameters maximizing the secrecy throughput. Our results revealed that by applying our versatile strategy, a larger feasible the reliability-security region and a higher maximum secrecy throughput are achieved.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

[3] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath Jr., "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May 2015.

[4] Y. Yang, W. Wang, H. Zhao, and L. Zhao, "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation," *J. Commun. Networks*, vol. 14, no. 4, pp. 374–384, Aug. 2012.

[5] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2435–2446, Nov. 2015.

[6] J. Hu, W. Yang, N. Yang, X. Zhou and Y. Cai, "On-off-based secure transmission design with outdated channel state information," *IEEE Trans. Veh. Technol.*, accepted to appear.

[7] C. C. Tan and N. C. Beaulieu, "On first-order Markov modeling for the Rayleigh fading channel," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2032–2040, Dec. 2000.

[8] Y. Yunchuan, W. Wenbo, Z. Hui, and Z. Long, "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation," *J. Commun. Networks*, vol. 14, no. 4, pp. 374–384, Aug. 2012.

[9] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1278–1290, May 2012.

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

[11] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, accepted to appear.

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

[13] X. Zhang, X. Zhou and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[14] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[15] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.

[16] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

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

[18] 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.

[19] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th Edition. Academic Press, 2007.

[20] J. I. Marcum, *Table of Q Functions*. Santa Monica, CA, USA: Rand Corporation, 1950.