# On-Off-Based Secure Transmission Design with Outdated Channel State Information

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

***Abstract*—We design new secure on-off transmission schemes in wiretap channels with outdated channel state information (CSI). In our design we consider not only the outdated CSI from the legitimate receiver but two distinct scenarios, depending on whether or not the outdated CSI from the eavesdropper is known at the transmitter. Under this consideration our schemes exploit the useful knowledge contained in the available outdated CSI, based on which the transmitter decides whether to transmit or not. We derive new closed-form expressions for the transmission probability, the connection outage probability, the secrecy outage probability, and the reliable and secure transmission probability to characterize the achievable performance. Based on these results, we present the optimal solutions that maximize the secrecy throughput under dual connection and secrecy outage constraints. Our analytical and numerical results offer detailed insights into the design of the wiretap coding parameters and the imposed outage constraints. We further show that allowing more freedom on the codeword transmission rate enables a larger feasible region of the dual outage constraints by exploiting the trade-off between reliability and security.**

***Index Terms*—Secure transmission, on-off scheme, outdated CSI, outage constraints, secrecy throughput.**

## I. Introduction

THE INHERENT openness of the wireless medium makes wireless data transmission difficult to be shielded from unintended recipients. As such, secure transmission over wireless channels becomes a critical issue in the design of wireless networks. Traditionally, security is viewed as an independent feature guaranteed through higher layer techniques, e.g., cryptographic protocols, assuming that an error-free physical layer link has already been established [1]. In large scale dynamic wireless networks, however, the high complexity of key distribution and management makes it difficult to achieve the required security level with cryptographic methods alone [2]. In contrast to cryptographic protocols, physical layer security exploits the statistics of the channel at the physical layer to protect wireless transmission against eavesdropping [3], [4]. Therefore, it has been widely recognized as a complement to cryptographic protocols for security enhancement and thus attracted enormous research efforts recently.

### A. Background

The information-theoretical foundation of physical layer security was laid down by Shannon's definition of perfect secrecy in [5]. Based on [5], [6] introduced the wiretap channel model as a basic framework for physical layer security. The results in [6] were subsequently generalized to the broadcast channel and the Gaussian channel in [7] and [8], respectively. These early studies revealed that if the eavesdropper's observation is a degraded version of the legitimate user's observation, it is possible to provide information-theoretically secure communication between the legitimate users while keeping the eavesdropper completely ignorant of secure messages.

A key assumption underpinning the information-theoretical contributions in [6]–[8] is that perfect channel state information (CSI) from both the legitimate receiver and the eavesdropper is available at the transmitter. However, this assumption may not be realistic since the uncertainty in CSI is a common factor that affects the performance of practical communication systems. In particular, if the eavesdropper is a passive user, knowing the CSI from the eavesdropper is almost impossible. Moreover, the perfect knowledge of the legitimate user's channel may not be easy to obtain at the transmitter in practice, due to the limitations incurred by signal processing techniques such as channel estimation errors, finite-rate feedback links, and outdated CSI (or delayed CSI).

Against this background, a growing body of research efforts have recently been devoted to examining the impact of imperfect CSI on physical layer security. Considering the practical passive eavesdropping scenario, [9]–[13] proposed transmit antenna selection schemes to enhance security in wiretap channels. Considering Gaussian-distributed errors produced by imperfect channel estimation at the legitimate receiver, [14]–[19] designed secure transmission schemes and investigated the achievable performance. It is worth mentioning that [19] successfully introduced on-off design to develop fixed-rate and variable-rate secure transmission schemes in the presence of channel estimation errors. Considering limited feedback constraints, [20]–[24] characterized the secrecy performance in multi-antenna systems and studied the optimal power allocation applied in artificial-noise-aided beamforming. Note



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) and Jiangsu provincial National Science Foundation (BK20150718). 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.2015.2477427

that [24] also adopted on-off design to develop the optimized artificial-noise-aided transmission scheme in limited feedback channels. Although [9]–[24] have developed signal processing techniques with passive eavesdropping, imperfect channel estimation and limited feedback constraints, the models and methods used in these papers cannot be used to address another practical environment where imperfect CSI is caused by the time delay of feedback link. This motivates us to develop new models and methods for physical layer security with outdated CSI.

### B. Motivation

Outdated CSI is a practical contributor to the uncertainty of channel knowledge at communication nodes. In a practical system with feedback delay from the receiver to the transmitter, the CSI obtained at the transmitter may be an outdated version of the actual CSI. As such, the obtained CSI cannot be directly used for secure transmission. Along this line there are limited studies in the literature [25], [26]. Specifically, [25] derived an upper bound on the secrecy rate loss by exploiting the Gauss-Markov fading spectrum to model the feedback delay, while [26] analyzed the effects of outdated CSI on the secrecy outage performance of multi-input single-output wiretap channels with transmit antenna selection. Notably, [25], [26] merely concentrated on the secrecy performance analysis, but have not presented detailed transmission design in the presence of outdated CSI.

It is well to be reminded that although the outdated CSI is not equivalent to the actual CSI, the temporal correlation between outdated CSI and actual CSI makes it possible for the transmitter to exploit some knowledge offered by the outdated CSI to perform secure transmission. Therefore, there arises a significant problem to be addressed: *"how can we take advantage of this benefit to design secure transmission schemes?"* Recall that the on-off design, as an efficient approach that guarantees transmission quality, has been successfully used to develop transmission schemes in the presence of channel estimation errors [19] and limited feedback constraints [24], respectively. Motivated by this, in this work we adopt the on-off design to develop secure transmission schemes in the presence of outdated CSI.

### C. Contributions

We develop new secure transmission schemes in the presence of outdated CSI by using on-off design to exploit the useful information existed in the outdated CSI. These schemes are designed for two distinct scenarios, depending on whether or not the eavesdropper is a legitimate user served by the transmitter. In *Scenario 1*, the eavesdropper is an active user (but not the intended receiver) and the outdated CSI from both the legitimate receiver and the eavesdropper is available at the transmitter. In *Scenario 2*, the eavesdropper is not a legitimate user and only the outdated CSI from the legitimate receiver is available at the transmitter. The on-off design adopted in our developed schemes allows transmission only when the channel qualities known at the transmitter satisfy some predetermined requirements [19], [24], [27], [28]. The rationale behind the on-off design is that transmission should be avoided when the quality of the intended receiver's channel is poor or the quality of the eavesdropper's channel is strong.

Our primary contributions are summarized as follows:

- We design new on-off transmission schemes in the presence of outdated CSI and then derive new closed-form expressions for the connection outage probability, the secrecy outage probability, and the reliable and secure transmission probability to quantify the achievable performance. Different from [19], [24], [28], for the first time we incorporate the reliable and secure transmission probability into the formulation of the throughput, forming the *secrecy throughput*. Notably, the secrecy throughput measures the average rate of the message which is successfully decoded at the legitimate receiver while being kept confidential to the eavesdropper.
- We determine new rate selection strategies that exploit the useful information existed in the outdated CSI. In these strategies, the codeword transmission rate is adaptively designed according to the feedback from the legitimate receiver. The secrecy rate is optimally selected to maximize the secrecy throughput subject to the constraints on the connection outage probability and secrecy outage probability. We present the optimal design for both Scenario 1 and *Scenario 2*.
- We reach an important conclusion that allowing more freedom on the codeword transmission rate enables the enhancement of the reliability level by exploiting the trade-off between reliability and security, since the codeword transmission rate without optimization leads to the poor reliability performance. We further show that this trade-off provides us with a profound extension in the feasible region of reliability constraint.

### D. Organization

The remainder of this paper is organized as follows. Section II details the outdated CSI model, the on-off transmission schemes and the wiretap codes design in wiretap channels. In Section III, we derive the exact expressions for the performance metrics and offer numerical results to investigate the secrecy performance. In Section IV, the optimized secrecy rates for each scenario are presented, and the illustrative numerical results are provided. Some discussions and concluding remarks are provided in Sections V and VI, respectively.

## II. Secure Transmission in the Presence of Outdated CSI

We consider a wiretap channel where the message transmitted from a source Alice to a destination Bob is intercepted by an eavesdropper Eve. We assume that Alice, Bob, and Eve are equipped with a single antenna each. Throughout this paper, we refer to the Alice-Bob channel as the main channel and refer to the Alice-Eve channel as the eavesdropper's channel. We assume that both channels are subject to Rayleigh fading. We also assume independent but non-identical distributions between the main channel and the eavesdropper's channel such that they have different average signal-to-noise ratios (SNRs).

Prior to data transmission, Alice requests Bob to feed back his instantaneous channel quality by sending pilot signals. Aided by the pilot signals, Bob estimates the main channel coefficient, $h_b$, and calculates the instantaneous received SNR as $\gamma_b = P_b|h_b|^2/\sigma_b^2$, where $P_b$ and $\sigma_b^2$ denote the average received signal power at Bob and the additive white Gaussian noise (AWGN) power at Bob, respectively; while Eve estimates the eavesdropper's channel coefficient, $h_e$, and calculates the instantaneous received SNR as $\gamma_e = P_e|h_e|^2/\sigma_e^2$, where $P_e$ and $\sigma_e^2$ denote the average received signal power at Eve and the AWGN power at Eve, respectively. Then Bob feeds back $\gamma_b$ to Alice to facilitate wiretap codes design. Whether or not Eve feeds back $\gamma_e$ depends on whether or not Eve is an active user of the network. Specifically, we consider two scenarios based on the availability of $\gamma_e$ in this work, as follows:

- *Scenario 1*: Eve is a non-passive eavesdropper such that $\gamma_e$ is fed back to Alice. This scenario represents the case where Eve is an active user of the network but is treated as a malicious eavesdropper when Alice performs secure transmission to Bob [29]–[31].
- *Scenario 2*: Eve is a passive eavesdropper such that $\gamma_e$ is not fed back to Alice. This scenario represents the case where Eve is an illegitimate user of the network [9]–[13].

We clarify that in both scenarios Eve is a regular user served by Alice and thus Eve's distance from Alice is known and the path loss exponent is known. That is, Alice always knows the average received SNR at Eve, $\bar{\gamma}_e$. Based on the feedback information, Alice calculates the instantaneous channel capacity of the main channel during pilot transmission as $C_b = \log_2(1+\gamma_b)$. Moreover, in *Scenario 1* Alice calculates the instantaneous channel capacity of the eavesdropper's channel capacity as $C_e = \log_2(1+\gamma_e)$; while in *Scenario 2* Alice calculates the average channel capacity of the eavesdropper's channel capacity as $\bar{C}_e = \log_2(1+\bar{\gamma}_e)$. Then Alice adaptively designs the wiretap codes based on $C_b$ and $C_e$ in *Scenario 1* but based on $C_b$ and $\bar{C}_e$ in *Scenario 2*.

### A. Outdated CSI

In this work, we concentrate on the practical wiretap channel where the CSI obtained at Alice is outdated. In the practice, the process of acquiring CSI at the transmitter may take a significant time duration for pilot transmission, channel estimation, and CSI feedback. This results in the fact that the channel coefficients during data transmission are not $h_b$ and $h_e$. As such, the CSI obtained at Alice is an imprecise version of the actual CSI, which causes the uncertainty in channel quality.

We first describe the uncertainty in the channel knowledge obtained at Alice in the wiretap channel. We define $\tilde{h}_b$ and $\tilde{h}_e$ as the $\tau_d$ time-delayed versions of $h_b$ and $h_e$, respectively. Using a Gauss-Markov process [32], we formulate $\tilde{h}_b$ and $\tilde{h}_e$ as

$$\tilde{h}_b = \rho_b h_b + \sqrt{1-\rho_b^2} w_b \tag{1}$$

and

$$\tilde{h}_e = \rho_e h_e + \sqrt{1-\rho_e^2} w_e, \tag{2}$$

respectively, where $w_b \sim \mathcal{CN}(0,1)$ and $w_e \sim \mathcal{CN}(0,1)$ are the channel-independent errors in the main channel and the eavesdropper's channel, respectively. Here, $\rho_b$ denotes the correlation coefficient between $\tilde{h}_b$ and $h_b$, while $\rho_e$ denotes the correlation coefficient between $\tilde{h}_e$ and $h_e$. In the Clark's fading model, $\rho_b$ and $\rho_e$ can be expressed as $\rho_b = J_0(2\pi f_b \tau_d)$ and $\rho_e = J_0(2\pi f_e \tau_d)$, where $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind, $f_b$ and $f_e$ are the maximum Doppler frequencies at Bob and Eve, respectively. In the Gaussian fading model, $\rho_b$ and $\rho_e$ can be expressed as $\rho_b = \exp(-\pi^2 f_b^2 \tau_d^2)$ and $\rho_e = \exp(-\pi^2 f_e^2 \tau_d^2)$, from which we find that $\rho_b$ and $\rho_e$ degrade monotonically to zero as $\tau_d$ increases. Since the Jakes model is widely adopted in the existing studies on mobile radios [32], in this work we use this model to perform the simulations in Section III-C, Section IV-C and Section V. Therefore, the received signals at Bob and Eve during data transmission are given by

$$y_b = \tilde{h}_b\sqrt{P_b}x + n_b = \left(\rho_b h_b + \sqrt{1-\rho_b^2} w_b\right)\sqrt{P_b}x + n_b \tag{3}$$

and

$$y_e = \tilde{h}_e\sqrt{P_e}x + n_e = \left(\rho_e h_e + \sqrt{1-\rho_e^2} w_e\right)\sqrt{P_e}x + n_e, \tag{4}$$

respectively, where $n_b \sim \mathcal{CN}\left(0,\sigma_b^2\right)$ and $n_e \sim \mathcal{CN}\left(0,\sigma_e^2\right)$ denote the AWGN at Bob and Eve, respectively. Based on (3) and (4), the instantaneous SNRs at Bob and Eve during data transmission are given by $\tilde{\gamma}_b = |\tilde{h}_b|^2 P_b/\sigma_b^2$ and $\tilde{\gamma}_e = |\tilde{h}_e|^2 P_e/\sigma_e^2$, respectively. Of course, $\tilde{\gamma}_b$ and $\tilde{\gamma}_e$ cannot be obtained at Alice.

### B. On-Off Schemes and Performance Metrics

We adopt Wyner's encoding strategy [6] for secure transmission in the presence of outdated CSI. Before each transmission block, Alice needs to choose two rate parameters for wiretap codes design, i.e., the codeword transmission rate, $R_b$, and the secrecy rate, $R_s$. The rate redundancy, $R_b - R_s$, provides secrecy against eavesdropping. We clarify that $R_b$ and $R_s$ hold constant over the duration of a block. In this work we use on-off schemes for *Scenario 1* and *Scenario 2*, as done in [19], [28], which are detailed as follows:

- On-off scheme for *Scenario 1*: Based on the feedback from Bob and Eve, Alice obtains the channel capacity of the main channel, $C_b$, and the channel capacity of the eavesdropper's channel $C_e$. As such, Alice uses $C_b$ and $C_e$ to design wiretap codes and performs data transmission only when $C_b - C_e > R_s$.
- On-off scheme for *Scenario 2*: Based on the feedback from Bob, Alice only obtains $C_b$. By aid of the statistic knowledge of the eavesdropper's channel, Alice uses $C_b$ and $\bar{C}_e$ to design wiretap codes and performs data transmission only when $C_b - \bar{C}_e > R_s$.

It is worthwhile to note that perfect connection and perfect secrecy between Alice and Bob cannot be guaranteed in the presence of outdated CSI for both cases. This is due to the uncertainty in channel knowledge, i.e., Alice has no knowledge of the actual main channel capacity given by $\tilde{C}_b = \log_2(1+\tilde{\gamma}_b)$ and the actual eavesdropper's channel

capacity given by $\tilde{C}_e = \log_2(1+\tilde{\gamma}_e)$. As such, the connection outage occurs when $\tilde{C}_b < R_b$, in which Bob is unable to decode the received codewords correctly. Mathematically, the connection outage probability, $p_{co}$, is defined as [19, Eq. (16)]

$$p_{co} = \Pr\left\{\tilde{C}_b < R_b \,|\text{transmission}\right\}. \tag{5}$$

Moreover, the secrecy outage occurs when $R_b - R_s < \tilde{C}_e$. Mathematically, the secrecy outage probability, $p_{so}$, is defined as [19, Eq. (15)]

$$p_{so} = \Pr\left\{R_b - R_s < \tilde{C}_e \,|\text{transmission}\right\}. \tag{6}$$

Note that both outage probabilities are conditioned upon a message being transmitted. These outage probabilities are of practical importance since the reliability level and the security level can be measured using these probabilities when the outdated CSI is in presence. However, from (5) and (6) we find that the connection outage event and the secrecy outage event are definitely not independent from each other, but related with $R_b$. To evaluate the combination of reliability and security, we resort to the successful (reliable and secure) transmission probability, $p_{rst}$, which is defined as

$$p_{rst} = \Pr\left\{\tilde{C}_b \geq R_b, R_b - R_s \geq \tilde{C}_e \,|\text{transmission}\right\}. \tag{7}$$

Notably, (7) is a novel formulation to characterize the reliability and security levels of transmission.

### C. Rate Selection Strategy

To exploit the useful knowledge existing in the outdated CSI, the strategy for the choice of $R_b$ and $R_s$ is explained as following: $R_b$ is adaptively designed according to the feedback from the legitimate receiver, while $R_s$ is optimally chosen and keeps constant over the transmission block. In other words, this is an adaptive-codeword-transmission-rate but fixed-secrecy-rate strategy. Since $C_b$ is the only knowledge obtained from Bob, it is convenient and natural for Alice to set $R_b = C_b$ to guarantee maximum rate redundancy against eavesdropping. This leads to the fact that $R_s$ is the only controllable parameter in the wiretap codes design. As such, $R_s$ is optimally chosen before data transmission and then kept constant during data transmission.

The aim of our design is to achieve the optimal secrecy throughput under the constraints of two outage probabilities. Here, the secrecy throughput, $\eta$, is defined as

$$\eta = p_{tx} p_{rst} R_s, \tag{8}$$

where $p_{tx}$ denotes the transmission probability and $p_{rst}$ is given by (7). *We highlight that the secrecy throughput in* (8) *is different from the throughput in [19], defined as* $p_{tx}(1-p_{co})R_s$. In (8), we introduce $p_{rst}$ into the formulation of the secrecy throughput. We clarify that the incorporation of $p_{rst}$ is reasonable and necessary for the assessment and improvement of reliability and security. Specifically, $p_{rst}$ jointly quantizes the reliability level and the security level of the secrecy throughput.

Using (8), our design aim is formulated as

$$\begin{aligned} \max_{R_s} \quad & \eta, \\ \text{subject to} \quad & p_{co} \leq \epsilon, p_{so} \leq \delta, \end{aligned} \tag{9}$$

where $\epsilon$ denotes the reliability constraint and $\delta$ denotes the security constraint. Note that solving the optimized $R_s$ in (9) can help us not only obtain good secrecy throughput performance but keep the reliability and security levels under control.

## III. Secrecy Performance with On-off Transmission Schemes

In this section, we analyze the secrecy performance for the two scenarios presented in Section II-B by exploiting the on-off transmission schemes. Specifically, we derive the closed-form expressions for the connection outage probability, the secrecy outage probability as well as the reliable and secure transmission probability defined in Section II-B. We then present the numerical results to examine the performance of the on-off transmission schemes with outdated CSI.

### A. Performance Analysis for Scenario 1

In this subsection, we consider *Scenario 1* and derive new expressions for the connection outage probability, the secrecy outage probability, the reliable and secure transmission probability. We then present the feasibility of the reliability constraint and the security constraint as well.

*1) $p_{tx_1}(R_s)$, $p_{co_1}(R_s)$, $p_{so_1}(R_s)$ and $p_{rst_1}(R_s)$:* In *Scenario 1*, Alice sets $R_b = C_b$ and performs data transmission only when $C_b - C_e \geq R_s$. The transmission probability in *Scenario 1* is derived as

$$\begin{aligned} p_{tx_1}(R_s) &= \Pr\{C_b - C_e \geq R_s\} \\ &= \Pr\left\{\gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\} \\ &= \int_0^\infty f_{\gamma_e}(\gamma_e) \left( \int_{2^{R_s}(1+\gamma_e)-1}^\infty f_{\gamma_b}(\gamma_b)\, d\gamma_b \right) d\gamma_e \\ &= \frac{\bar{\gamma}_b}{\bar{\gamma}_b + 2^{R_s}\bar{\gamma}_e} \exp\left(-\frac{2^{R_s}-1}{\bar{\gamma}_b}\right). \end{aligned} \tag{10}$$

We note that (10) can be obtained by using the probability density functions (PDFs) of $\gamma_b$ and $\gamma_e$. In this work, we assume that both the main channel and the eavesdropper's channel are subject to Rayleigh fading, such that the PDF of $\gamma_b$ is $f_{\gamma_b}(\gamma_b) = \exp(-\gamma_b/\bar{\gamma}_b)/\bar{\gamma}_b$ and the PDF of $\gamma_e$ is $f_{\gamma_e}(\gamma_e) = \exp(-\gamma_e/\bar{\gamma}_e)/\bar{\gamma}_e$ [19], where $\bar{\gamma}_b = \mathbb{E}\left[h_b^2\right] P_b/\sigma_b^2$ denotes the average SNR at Bob and $\bar{\gamma}_e = \mathbb{E}\left[h_e^2\right] P_e/\sigma_e^2$ denotes the average SNR at Eve.

The connection outage occurs when $\tilde{C}_b < C_b$. As such, the connection outage probability in *Scenario 1* is given by

$$p_{co_1}(R_s) = \Pr\left\{\tilde{C}_b < C_b \,|C_b - C_e \geq R_s\right\}. \tag{11}$$

Based on the cumulative density distribution (CDF) of a non-central chi-square distributed variable, we derive $p_{co_1}(R_s)$ as

$$\begin{aligned} p_{co_1}(R_s) =& 1 - \frac{\bar{\gamma}_b + 2^{R_s}\bar{\gamma}_e}{\bar{\gamma}_b} \exp\left(-\frac{\left(1+\rho_b^2\right)\left(2^{R_s}-1\right)}{\left(1-\rho_b^2\right)\bar{\gamma}_b}\right) \\ &\times \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\rho_b^{2(n+k)}\left(1-\rho_b^2\right)\Gamma\left(n+2k+1\right)}{k!2^{n+2k+1}\Gamma\left(n+k+1\right)} \\ &\times \sum_{m=0}^{n+2k}\sum_{q=0}^{m} \frac{\left(2^{R_s}-1\right)^{m-q}2^{m+qR_s}}{(m-q)!\left(\left(1-\rho_b^2\right)\bar{\gamma}_b\right)^m\bar{\gamma}_e} \\ &\times \left(\frac{\left(1-\rho_b^2\right)\bar{\gamma}_b\bar{\gamma}_e}{\left(1-\rho_b^2\right)\bar{\gamma}_b + 2^{R_s+1}\bar{\gamma}_e}\right)^{q+1}, \end{aligned} \tag{12}$$

where $\Gamma(\cdot)$ is the Gamma function defined in [33, Eq. (8.310.1)]. The proof is given in Appendix A.

The secrecy outage occurs when $C_b - R_s < \tilde{C}_e$. As such, the secrecy outage probability in *Scenario 1* is given by

$$p_{so_1}(R_s) = \Pr\left\{C_b - R_s < \tilde{C}_e \,|C_b - C_e \geq R_s\right\}. \tag{13}$$

We derive $p_{so_1}(R_s)$ as

$$p_{so_1}(R_s) = \frac{\bar{\gamma}_b + 2^{R_s}\bar{\gamma}_e}{\bar{\gamma}_b} \exp\left(\frac{2^{R_s}-1}{\bar{\gamma}_b}\right)(\ell_1 - \ell_2), \tag{14}$$

where $\ell_1$ is

$$\begin{aligned} \ell_1 =& \exp\left(-\frac{2^{-R_s}-1}{\left(1-\rho_e^2\right)\bar{\gamma}_e}\right)\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{\rho_e^{2(n+k)}\left(1-\rho_e^2\right)}{\Gamma\left(k+1\right)\left(\left(1-\rho_e^2\right)\bar{\gamma}_e\right)^k} \\ &\times \sum_{q=0}^{k}\binom{k}{q}\frac{\left(1-2^{R_s}\right)^{k-q}}{2^{kR_s}\bar{\gamma}_b}\left(\frac{\left(1-\rho_e^2\right)2^{R_s}\bar{\gamma}_b\bar{\gamma}_e}{\bar{\gamma}_b + \left(1-\rho_e^2\right)2^{R_s}\bar{\gamma}_e}\right)^{q+1} \\ &\times \Gamma\left(q+1, \frac{\bar{\gamma}_b + \left(1-\rho_e^2\right)2^{R_s}\bar{\gamma}_e}{\left(1-\rho_e^2\right)2^{R_s}\bar{\gamma}_b\bar{\gamma}_e}\left(2^{R_s}-1\right)\right), \end{aligned} \tag{15}$$

$\ell_2$ is

$$\begin{aligned} \ell_2 =& \exp\left(-\frac{2^{1-R_s}-2}{\left(1-\rho_e^2\right)\bar{\gamma}_e}\right)\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{\rho_e^{2(n+k)}\left(1-\rho_e^2\right)}{k!\left(\left(1-\rho_e^2\right)\bar{\gamma}_e\right)^k} \\ &\times \sum_{m=0}^{n+k}\sum_{q=0}^{k+m}\binom{k+m}{q}\frac{\left(2^{-R_s}-1\right)^{k+m-q}2^{-qR_s}}{m!\left(\left(1-\rho_e^2\right)\bar{\gamma}_e\right)^m\bar{\gamma}_b} \\ &\times \Gamma\left(q+1, \frac{2^{1-R_s}\bar{\gamma}_b + \left(1-\rho_e^2\right)\bar{\gamma}_e}{\left(1-\rho_e^2\right)\bar{\gamma}_b\bar{\gamma}_e}\left(2^{R_s}-1\right)\right) \\ &\times \left(\frac{\left(1-\rho_e^2\right)\bar{\gamma}_b\bar{\gamma}_e}{2^{1-R_s}\bar{\gamma}_b + \left(1-\rho_e^2\right)\bar{\gamma}_e}\right)^{q+1}, \end{aligned} \tag{16}$$

and $\Gamma(\cdot,\cdot)$ is the incomplete Gamma function defined in [33, Eq. (8.352.2)]. The proof is given in Appendix B.

The successful transmission occurs when both $\tilde{C}_b \geq C_b$ and $C_b - R_s \geq \tilde{C}_e$ are satisfied simultaneously. As such, the reliable and secure transmission probability in *Scenario 1* is given by

$$p_{rst_1}(R_s) = \Pr\left\{\tilde{C}_b \geq C_b, C_b - R_s \geq \tilde{C}_e \,|C_b - C_e \geq R_s\right\}. \tag{17}$$

We derive $p_{rst_1}(R_s)$ as

$$p_{rst_1}(R_s) = \frac{\bar{\gamma}_b + 2^{R_s}\bar{\gamma}_e}{\bar{\gamma}_b}\exp\left(\frac{2^{R_s}-1}{\bar{\gamma}_b}\right)(\ell_3 - \ell_4 - \ell_5), \tag{18}$$

where $\ell_3$ is

$$\begin{aligned} \ell_3 =& \sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{\rho_b^{2(n+k)}\left(1-\rho_b^2\right)}{\Gamma\left(k+1\right)\Gamma\left(n+k+1\right)2^{n+2k+1}} \\ &\times \Gamma\left(n+2k+1, \frac{2\left(2^{R_s}-1\right)}{\left(1-\rho_b^2\right)\bar{\gamma}_b}\right), \end{aligned} \tag{19}$$

$\ell_4$ is

$$\begin{aligned} \ell_4 =& \exp\left(-\frac{2^{-R_s}-1}{\bar{\gamma}_e}\right)\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{\rho_b^{2(n+k)}\left(1-\rho_b^2\right)}{\Gamma\left(k+1\right)\Gamma\left(n+k+1\right)} \\ &\times \Gamma\left(n+2k+1, \frac{\left(2^{R_s+1}\bar{\gamma}_e + \left(1-\rho_b^2\right)\bar{\gamma}_b\right)}{\left(2^{R_s}-1\right)^{-1}\left(1-\rho_b^2\right)2^{R_s}\bar{\gamma}_b\bar{\gamma}_e}\right) \\ &\times \left(\frac{2^{R_s}\bar{\gamma}_e}{2^{R_s+1}\bar{\gamma}_e + \left(1-\rho_b^2\right)\bar{\gamma}_b}\right)^{n+2k+1}, \end{aligned} \tag{20}$$

and $\ell_5 = \ell_6 - \ell_7$, where $\ell_6$ and $\ell_7$ are given at the top of next page. The proof is given in Appendix C.

***Remark 1:*** We clarify that the connection outage probability is merely affected by $\rho_b$, as indicated by (12), and the secrecy outage probability is merely affected by $\rho_e$, as indicated by (14). This reveals that in *Scenario 1*, the reliability level depends on the outdated CSI of the main channel, while the security level depends on the outdated CSI of the eavesdropper's channel.

*2) Feasibility of Constraints:* We now investigate the feasibility of the reliability constraint and the security constraint. Using the mathematical software package to take the first derivative of $p_{co_1}(R_s)$ in (12), we find that $p_{co_1}(R_s)$ is an increasing function of $R_s$. When $R_s \to 0$, $p_{co_1}(R_s)$ achieves its lower bound, $p_{co_1,LB}$. We obtain $p_{co_1,LB}$ as

$$\begin{aligned} p_{co_1,LB} =& 1 - \sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{\rho_b^{2(n+k)}\Gamma\left(n+2k+1\right)}{\Gamma\left(k+1\right)\Gamma\left(n+k+1\right)2^{n+2k+1}} \\ &\times \sum_{m=0}^{n+2k}\frac{\left(1-\rho_b^2\right)^2\left(\bar{\gamma}_b + \bar{\gamma}_e\right)2^m\bar{\gamma}_e^m}{\left(2\bar{\gamma}_e + \left(1-\rho_b^2\right)\bar{\gamma}_b\right)^{m+1}}. \end{aligned} \tag{23}$$

As such, the feasible range of the reliability constraint in *Scenario 1* is given by

$$p_{co_1,LB} < \epsilon \leq 1. \tag{24}$$

We then take the first derivative of $p_{so_1}(R_s)$ in (14) and find that $p_{so_1}(R_s)$ is also an increasing function of $R_s$. When $R_s \to 0$, $p_{so_1}(R_s)$ achieves its lower bound, $p_{so_1,LB}$. We obtain $p_{so_1,LB}$ as

$$\begin{aligned} p_{so_1,LB} =& \frac{\bar{\gamma}_b + \bar{\gamma}_e}{\bar{\gamma}_b}\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\left(\frac{\rho_e^{2(n+k)}\left(1-\rho_e^2\right)^2\bar{\gamma}_e\bar{\gamma}_b^k}{\left(\bar{\gamma}_b + \left(1-\rho_e^2\right)\bar{\gamma}_e\right)^{k+1}}\right. \\ &\left. - \sum_{m=0}^{n+k}\binom{m+k}{m}\frac{\rho_e^{2(n+k)}\left(1-\rho_e^2\right)^2\bar{\gamma}_e\bar{\gamma}_b^{m+k}}{\left(2\bar{\gamma}_b + \left(1-\rho_e^2\right)\bar{\gamma}_e\right)^{m+k+1}}\right). \end{aligned} \tag{25}$$

$$\ell_6 = \exp\left(-\frac{2^{-R_s}-1}{(1-\rho_e^2)\,\bar{\gamma}_e}\right)\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\sum_{s=0}^{\infty}\sum_{t=0}^{\infty}\frac{\rho_b^{2(n+k)}\rho_e^{2(s+t)}\left(1-\rho_b^2\right)\left(1-\rho_e^2\right)\left(\left(1-\rho_e^2\right)\bar{\gamma}_e\right)^{n+2k-t+1}}{k!\Gamma\left(n+k+1\right)t!(2\left(1-\rho_e^2\right)\bar{\gamma}_e+2^{-R_s}\left(1-\rho_b^2\right)\bar{\gamma}_b)^{n+2k+1}}\sum_{q=0}^{t}\frac{t!\left(2^{-R_s}-1\right)^{t-q}}{q!\,(t-q)!}$$
$$\times\left(\frac{2^{-R_s}\left(1-\rho_b^2\right)\left(1-\rho_e^2\right)\bar{\gamma}_b\bar{\gamma}_e}{2\left(1-\rho_e^2\right)\bar{\gamma}_e+2^{-R_s}\left(1-\rho_b^2\right)\bar{\gamma}_b}\right)^{q}\Gamma\left(n+2k+q+1,\frac{2\left(1-\rho_e^2\right)\bar{\gamma}_e+2^{-R_s}\left(1-\rho_b^2\right)\bar{\gamma}_b}{\left(2^{R_s}-1\right)^{-1}\left(1-\rho_b^2\right)\left(1-\rho_e^2\right)\bar{\gamma}_b\bar{\gamma}_e}\right), \tag{21}$$

$$\ell_7 = \exp\left(-\frac{2^{1-R_s}-2}{(1-\rho_e^2)\,\bar{\gamma}_e}\right)\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\sum_{s=0}^{\infty}\sum_{t=0}^{\infty}\frac{\rho_b^{2(n+k)}\rho_e^{2(s+t)}\left(1-\rho_b^2\right)\left(1-\rho_e^2\right)}{\left(2\left(1-\rho_e^2\right)\bar{\gamma}_e+2^{1-R_s}\left(1-\rho_b^2\right)\bar{\gamma}_b\right)^{n+2k+1}}\sum_{m=0}^{s+t}\sum_{q=0}^{t+m}\frac{\left(\left(1-\rho_e^2\right)\bar{\gamma}_e\right)^{n+2k-t-m+1}}{\Gamma\left(n+k+1\right)(t+m-q)!}$$
$$\times\frac{\left(2^{-R_s}-1\right)^{t+m-q}}{((t+m)!)^{-1}k!t!m!q!}\left(\frac{2^{-R_s}\left(1-\rho_b^2\right)\left(1-\rho_e^2\right)\bar{\gamma}_b\bar{\gamma}_e}{2\left(1-\rho_e^2\right)\bar{\gamma}_e+2^{1-R_s}\left(1-\rho_b^2\right)\bar{\gamma}_b}\right)^{q}\Gamma\left(n+2k+q+1,\frac{2\left(1-\rho_e^2\right)\bar{\gamma}_e+2^{1-R_s}\left(1-\rho_b^2\right)\bar{\gamma}_b}{\left(2^{R_s}-1\right)^{-1}\left(1-\rho_b^2\right)\left(1-\rho_e^2\right)\bar{\gamma}_b\bar{\gamma}_e}\right). \tag{22}$$

Accordingly, we obtain the feasible range of the security constraint in *Scenario 1* as

$$p_{so_1,LB} < \delta \leq 1. \tag{26}$$

We highlight that in *Scenario 1* the reliability constraint and the security constraint are feasible only when (24) and (26) are satisfied.

### *B. Performance Analysis for Scenario 2*

In this subsection, we concentrate on *Scenario 2*. New closed-form expressions are derived for the transmission probability, connection outage probability, secrecy outage probability, reliable and secure transmission probability, based on which we evaluate the feasibility of the reliability and security constraints.

*1) $p_{tx_2}(R_s)$, $p_{co_2}(R_s)$, $p_{so_2}(R_s)$, and $p_{rst_2}(R_s)$:* In *Scenario 2*, Alice has no knowledge of $C_e$. As such, Alice sets $R_b = C_b$ and performs secure transmission only when $C_b - \bar{C}_e \geq R_s$. The transmission probability in *Scenario 2* is derived as

$$\begin{aligned} p_{tx_2}(R_s) &= \Pr\left\{C_b - \bar{C}_e \geq R_s\right\} \\ &= \Pr\left\{\gamma_b \geq 2^{R_s}\left(1+\bar{\gamma}_e\right)-1\right\} \\ &= \int_{2^{R_s}(1+\bar{\gamma}_e)-1}^{\infty} f_{\gamma_b}(\gamma_b)\,d\gamma_b \\ &= \exp\left(-\frac{2^{R_s}\left(1+\bar{\gamma}_e\right)-1}{\bar{\gamma}_b}\right). \end{aligned} \tag{27}$$

The connection outage probability in *Scenario 2* is given by

$$p_{co_2}(R_s) = \Pr\left\{\tilde{C}_b < C_b \,\middle|\, C_b - \bar{C}_e \geq R_s\right\}. \tag{28}$$

Applying the CDF of a non-central chi-square distributed variable, $p_{co_2}(R_s)$ is derived as

$$\begin{aligned} p_{co_2}(R_s) =& 1-\exp\left(\frac{2^{R_s}\left(1+\bar{\gamma}_e\right)-1}{\bar{\gamma}_b}\right)\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{1}{\Gamma\left(k+1\right)} \\ &\times\Gamma\left(n+2k+1,\frac{2^{R_s+1}\left(1+\bar{\gamma}_e\right)-2}{\left(1-\rho_b^2\right)\bar{\gamma}_b}\right) \\ &\times\left(\frac{1}{2}\right)^{n+2k+1}\frac{\rho_b^{2(n+k)}\left(1-\rho_b^2\right)}{\Gamma\left(n+k+1\right)}. \end{aligned} \tag{29}$$

The secrecy outage probability in *Scenario 2* is given by

$$p_{so_2}(R_s) = \Pr\left\{C_b - R_s < \tilde{C}_e \,\middle|\, C_b - \bar{C}_e \geq R_s\right\}. \tag{30}$$

Using the statistics of $\gamma_b$ and $\tilde{\gamma}_e$, we derive $p_{so_2}(R_s)$ as

$$p_{so_2}(R_s) = \frac{2^{R_s}\bar{\gamma}_e\exp(-1)}{2^{R_s}\bar{\gamma}_e+\bar{\gamma}_b}. \tag{31}$$

The reliable and secure transmission probability in *Scenario 2* is given by

$$p_{rst_2}(R_s) = \Pr\left\{\tilde{C}_b \geq C_b, C_b - R_s \geq \tilde{C}_e \,\middle|\, C_b - \bar{C}_e \geq R_s\right\}. \tag{32}$$

We derive $p_{rst_2}(R_s)$ as

$$p_{rst_2}(R_s) = \exp\left(\frac{2^{R_s}\left(1+\bar{\gamma}_e\right)-1}{\bar{\gamma}_b}\right)\left(\ell_8-\ell_9\right), \tag{33}$$

where $\ell_8$ is

$$\begin{aligned} \ell_8 =& \sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{\rho_b^{2(n+k)}\left(1-\rho_b^2\right)}{\Gamma\left(k+1\right)\Gamma\left(n+k+1\right)}\left(\frac{1}{2}\right)^{n+2k+1} \\ &\times\Gamma\left(n+2k+1,\frac{2\left(2^{R_s+1}\left(1+\bar{\gamma}_e\right)-2\right)}{\left(1-\rho_b^2\right)\bar{\gamma}_b}\right), \end{aligned} \tag{34}$$

and $\ell_9$ is

$$\begin{aligned} \ell_9 =& \exp\left(-\frac{2^{-R_s}-1}{\bar{\gamma}_e}\right)\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{\rho_b^{2(n+k)}\left(1-\rho_b^2\right)}{\Gamma\left(k+1\right)\Gamma\left(n+k+1\right)} \\ &\times\Gamma\left(n+2k+1,\frac{\left(2^{R_s+1}\bar{\gamma}_e+\left(1-\rho_b^2\right)\bar{\gamma}_b\right)\left(\bar{\gamma}_b\bar{\gamma}_e\right)^{-1}}{\left(2^{R_s}\left(1+\bar{\gamma}_e\right)-1\right)^{-1}2^{R_s}\left(1-\rho_b^2\right)}\right) \\ &\times\left(\frac{2^{R_s}\bar{\gamma}_e}{2^{R_s+1}\bar{\gamma}_e+\left(1-\rho_b^2\right)\bar{\gamma}_b}\right)^{n+2k+1}. \end{aligned} \tag{35}$$

***Remark 2:*** Based on (29) and (31), we find that the connection outage probability is only affected by $\rho_b$ but the secrecy outage probability is not influenced by either $\rho_b$ or $\rho_e$. This reveals that in *Scenario 2* the outdated CSI only influences the reliability level.

*2) Feasibility of Constraints:* We next examine the feasibility of the reliability constraint and the security constraint. Using the mathematical software package to take the first-order derivative of $p_{co_2}(R_s)$ in (29), we find that $p_{co_2}(R_s)$ is an increasing function of $R_s$. When $R_s \to 0$, $p_{co_2}(R_s)$ achieves its lower bound, $p_{co_2,LB}$, which is derived as

$$p_{co_2,LB} = 1 - \exp\left(\frac{\bar{\gamma}_e}{\bar{\gamma}_b}\right) \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\rho^{2(n+k)}\left(1-\rho^2\right)}{\Gamma(k+1)\,\Gamma(n+k+1)} \times \left(\frac{1}{2}\right)^{n+2k+1} \Gamma\left(n+2k+1, \frac{2\bar{\gamma}_e}{(1-\rho^2)\,\bar{\gamma}_b}\right). \tag{36}$$

Therefore, the feasible range of the reliability constraint in *Scenario 2* is given by

$$p_{co_2,LB} < \epsilon \leq 1. \tag{37}$$

Next, by observing (31) we see that $p_{so_2}(R_s)$ is also an increasing function of $R_s$. When $R_s \to 0$, $p_{so_2}(R_s)$ achieves its lower bound, $p_{so_2,LB}$, given by

$$p_{so_2,LB} = \frac{\bar{\gamma}_e \exp(-1)}{\bar{\gamma}_e + \bar{\gamma}_b}. \tag{38}$$

Thus, the feasible range of the security constraint in *Scenario 2* is obtained as

$$p_{so_2,LB} < \delta \leq 1. \tag{39}$$

It is worthwhile to note that in *Scenario 2* the reliability constraint and the security constraint are feasible only when (37) and (39) are satisfied.

### C. Numerical Results

We present numerical results in this subsection to examine the performance of the on-off transmission schemes. We clarify that the infinitive summations in our derived closed-form expressions can be perfectly approximated with finite summations (usually first 10 terms in the summations give an accurate approximation). The simulation settings are as follows, unless specified otherwise: The average received SNR at Bob is assumed to be $P_b/\sigma_b^2 = 10$ dB, while the average received SNR at Eve is assumed to be $P_e/\sigma_e^2 = 0$ dB. In each simulation trial, the main channel coefficient and the eavesdropper's channel coefficient are randomly generated using an i.i.d. complex Gaussian distribution with zero mean and unit variance. The temporal correlation parameters of the two channel coefficients are assumed to follow the Clarke's model and are characterized by $\rho_b = J_0(2\pi f_b \tau_d)$ and $\rho_e = J_0(2\pi f_e \tau_d)$, respectively. All the results to be shown are averaged over 10,000 channel trials. It is evident from Figs. 1, 2 and 3 that the Monte Carlo simulation points, marked by '$*$', match precisely with the analytical curves, which demonstrates the accuracy of our analysis.

Fig. 1 plots the connection outage probability versus $R_s$ for two scenarios with different values of $\rho_b$. In this figure, $p_{co_1}(R_s)$ and $p_{co_2}(R_s)$ are generated from (12) and (29), respectively. We first observe that $p_{co_1}(R_s)$ and $p_{co_2}(R_s)$ increase with $R_s$. This is due to the fact that an increasing $R_s$ requires a higher $C_b$ to satisfy the transmission condition.

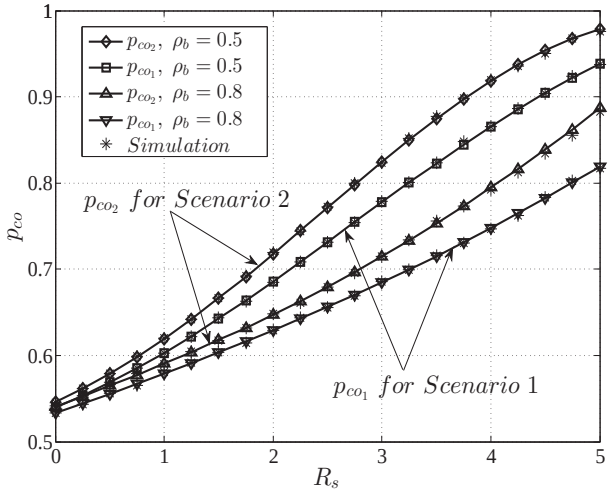


Fig. 1. Connection outage probability versus $R_s$ with outdated CSI for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

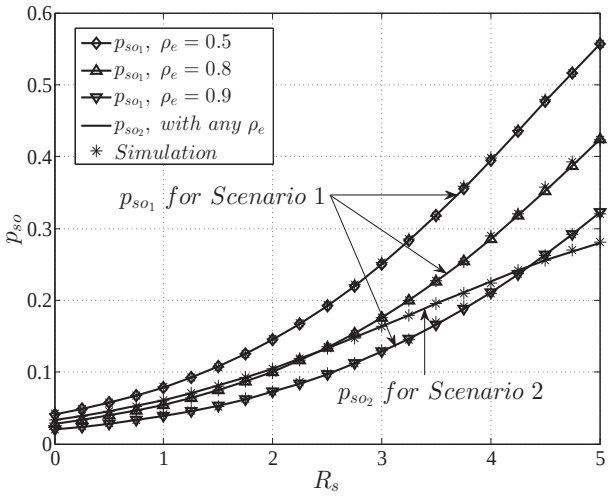


Fig. 2. Secrecy outage probability versus $R_s$ with outdated CSI for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

Notably, a higher $C_b$ leads to a higher probability that $\tilde{C}_b$ is lower than $C_b$, due to the characteristics of Gauss-Markov process. Second, we observe that $p_{co_1}(R_s)$ and $p_{co_2}(R_s)$ increase when $\rho_b$ decreases. This observation is not surprising since the uncertainty in the main channel quality increases as $\rho_b$ decreases, which results in a poorer reliability. Third, we observe that $p_{co_2}(R_s)$ is higher than $p_{co_1}(R_s)$ for the same $\rho_b$. This is due to the fact that the transmission condition in *Scenario 2*, $C_b \geq \bar{C}_e + R_s$, is stricter than that in *Scenario 1*, $C_b \geq C_e + R_s$. Thus, a higher $C_b$ is required in *Scenario 2*, which results in the worse reliability. Fourth, we observe that both $p_{co_1}(R_s)$ and $p_{co_2}(R_s)$ are always greater than 0.5, which implies that the reliability constraint should be loose in the on-off transmission schemes.

Fig. 2 plots the secrecy outage probability versus $R_s$ for two scenarios with different values of $\rho_e$. In this figure, $p_{so_1}(R_s)$ and $p_{so_2}(R_s)$ are generated from (14) and (31), respectively.

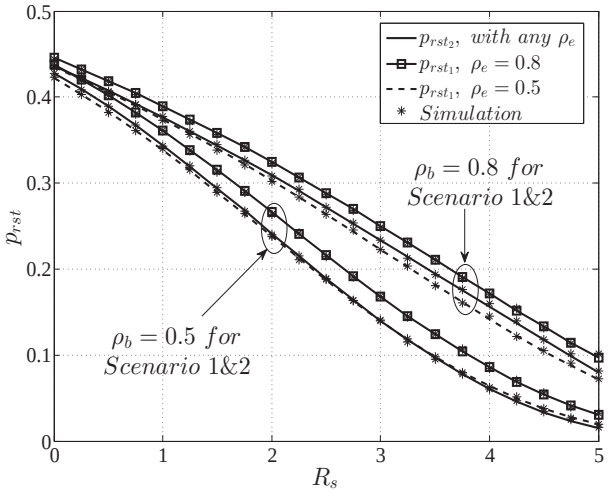


Fig. 3. Reliable and secure transmission probability versus $R_s$ with outdated CSI for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

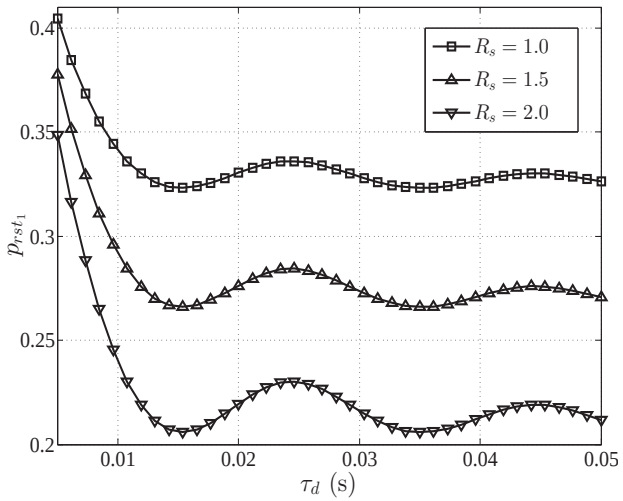


Fig. 4. Reliable and secure transmission probability versus $\tau_d$ for $\overline{\gamma}_b = 10$ dB, $\overline{\gamma}_e = 0$ dB, $v_b = v_e = 30$ km/h and $f_c = 900$ MHz in *Scenario 1*.

First, we observe that $p_{so_1}(R_s)$ and $p_{so_2}(R_s)$ increase as $R_s$ increases. This is due to the fact that the rate redundancy, $C_b - R_s$, decreases with $R_s$ and a lower rate redundancy leads to a higher probability that $\tilde{C}_e$ is higher than the rate redundancy. We then find that $p_{so_2}(R_s)$ is not influenced by the value of $\rho_e$ and different behavior of $p_{so_1}(R_s)$ is observed depending on the value of $\rho_e$, as indicated by (31). When $\rho_e$ is not sufficiently high (e.g. $\rho_e \leq 0.5$), $p_{so_1}(R_s)$ is always higher than $p_{so_2}(R_s)$; however, when $\rho_e$ is sufficiently high (e.g. $\rho_e > 0.9$), the opposite happens. From a design perspective, this observation implies that $C_e$ should be used for transmission design only when $\rho_e$ is high; otherwise directly using $\bar{C}_e$ is a better choice for security enhancement. Moreover, we find that $p_{so_1}(R_s)$ and $p_{so_2}(R_s)$ are smaller than 0.1 for low $R_s$, which implies that the security constraint can be sufficiently strict in the on-off transmission schemes.

Fig. 3 plots the reliable and secrecy transmission probability versus $R_s$ for two scenarios with different values of $\rho_b$ and $\rho_e$. In this figure, $p_{rst_1}(R_s)$ and $p_{rst_2}(R_s)$ are generated from (18) and (33), respectively. We first observe that $p_{rst_1}(R_s)$ and $p_{rst_2}(R_s)$ decrease as $R_s$ increases. This is due to the fact that increasing $R_s$ strengthens the transmission condition (requiring higher $C_b$), which leads to a lower probability that $\tilde{C}_b$ is higher than $C_b$ while the rate redundancy is higher than $\tilde{C}_e$. We also observe that $p_{rst_1}(R_s)$ and $p_{rst_2}(R_s)$ decrease when $\rho_b$ decreases. Moreover, for a fixed $\rho_b$ in *Scenario 1*, $p_{rst_1}(R_s)$ also decreases when $\rho_e$ decreases. This is because that the uncertainty in the main and eavesdropper's channel quality increases as $\rho_b$ and $\rho_e$ decrease, which results in poorer reliability and security levels. Furthermore, we observe that for a fixed $\rho_b$, when $\rho_e$ is high (e.g. $\rho_e = 0.8$), $p_{rst_1}(R_s)$ is higher than $p_{rst_2}(R_s)$; but when $\rho_e$ is low (e.g. $\rho_e = 0.5$), $p_{rst_1}(R_s)$ is lower than $p_{rst_2}(R_s)$. This observation demonstrates that in terms of the reliable and secrecy transmission probability, a sufficiently high $\rho_e$ is required to guarantee that *Scenario 1* performs better than *Scenario 2*.

Fig. 4 plots the reliable and secure transmission probability versus $\tau_d$ for *Scenario 1* with different values of $R_s$. The correlation coefficients are generated by the Clark's fading model with $v_b = v_e = 30$ km/h and $f_c = 900$ MHz. We first observe that $p_{rst_1}(R_s)$ is not a monotony decrease function of $\tau_d$. In particular, we find that $p_{rst_1}(R_s)$ decreases fast before $\tau_d$ increases to 10 ms. However, when $\tau_d$ is sufficiently large, i.e., $\tau_d > 10$ ms, $p_{rst_1}(R_s)$ starts to fluctuate around a certain value and does not decrease further. This observation is not surprising since the absolute values of $\rho_b$ and $\rho_e$, generated by the Clark's fading model, fluctuate in the large delay regime. Moreover, we observe that for a fixed $\tau_d$, $p_{rst_1}(R_s)$ decreases as $R_s$ increases, which has been explained in the descriptions of Fig. 3. Similarly, we conclude that $p_{rst_2}(R_s)$ versus $\tau_d$ for *Scenario 2* has a similar conclusion. The detailed illustrations for *Scenario 2* are omitted in this subsection to avoid redundancy.

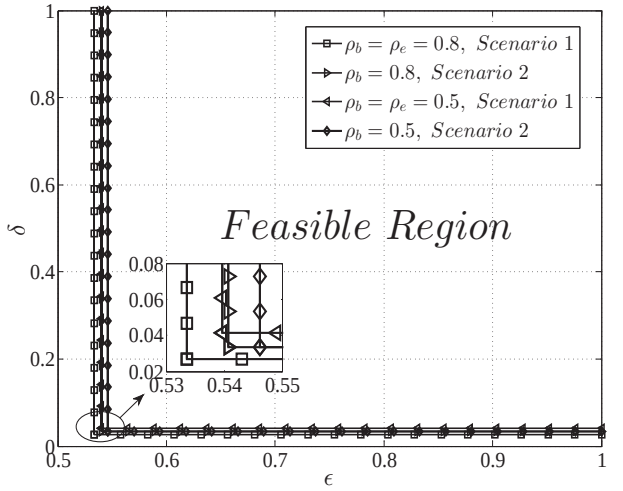


Fig. 5. Feasible security constraint versus feasible reliability constraint with outdated CSI for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

Fig. 5 plots the feasible security constraint versus the

feasible reliability constraint for both scenarios. In this figure, $p_{co_1,LB}$, $p_{so_1,LB}$, $p_{co_2,LB}$, and $p_{so_2,LB}$ are generated from (23), (25), (36), and (38), respectively. For each scenario with specifical $\rho_b$ and $\rho_e$ (only $\rho_e$ in *Scenario 2*), the feasible region of $\epsilon$ and $\delta$ lies in the region above the corresponding curve. First, we observe that in both *Scenario 1* and *Scenario 2* increasing $\rho_b$ leads to the extension of the feasible region. Second, we observe that the feasible region in *Scenario 2* is not influenced by $\rho_e$; while in *Scenario 1* we observe the extension in the feasible region when $\rho_e$ increases. Third, we observe that for the same $\rho_b$, *Scenario 1* enables higher reliability level than *Scenario 2*. However, in terms of the security level, whether *Scenario 1* performs better or not depends on the value of $\rho_e$. In particular, *Scenario 1* enables higher security level when $\rho_e$ is high (e.g. $\rho_e = 0.8$); while *Scenario 2* enables higher security level when $\rho_e$ is low(e.g. $\rho_e = 0.5$). Fourth, we observe that the feasible regions are strictly restricted at the right side of $\epsilon = 0.5$, which implies that this transmission design ignores the system reliability and can be only applied for the systems where the reliability is not seen as important.

## IV. Secure Transmission Design

In this section, we first investigate the optimal solutions for $R_s$ meeting (9) for each scenario, based on which we then present numerical results to investigate the impact of the dual outage constraints on the secrecy throughput in both scenarios.

### A. Optimized $R_s$ for Scenario 1

In *Scenario 1*, the secrecy throughput is given by

$$\eta_1(R_s) = p_{tx_1}(R_s)\, p_{rst_1}(R_s)\, R_s. \tag{40}$$

Mathematically, we express $S_1$ as

$$S_1 = \underset{R_s}{\operatorname{argmax}} \quad \eta_1(R_s). \tag{41}$$

Using the mathematical software package to take the first-order derivative of $\eta_1(R_s)$ with respect to $R_s$, we find that $\partial\eta_1(R_s)/\partial R_s$ is first positive and then negative, which confirms that without dual outage constraints there is a unique solution to $S_1$, which achieves the maximum $\eta_1(R_s)$.

Based on the feasibility for the dual outage constraints presented in (24) and (26), we express $S_2$ and $S_3$ as

$$S_2 = \{R_s \,|p_{co_1}(R_s) = \epsilon\}, \tag{42}$$

and

$$S_3 = \{R_s \,|p_{so_1}(R_s) = \delta\}, \tag{43}$$

respectively. As mentioned in Section III-A, both $p_{co_1}(R_s)$ and $p_{so_1}(R_s)$ are monotonous increasing functions of $R_s$, which guarantees that both (42) and (43) each have a unique solution.

Although the closed-form solutions for $S_1$, $S_2$, and $S_3$ are mathematically intractable, we are able to obtain them using a numerical method, e.g., bisection method. Based on above results, we present the optimal $R_s$ that meets (9) in *Scenario 1* in the following proposition.

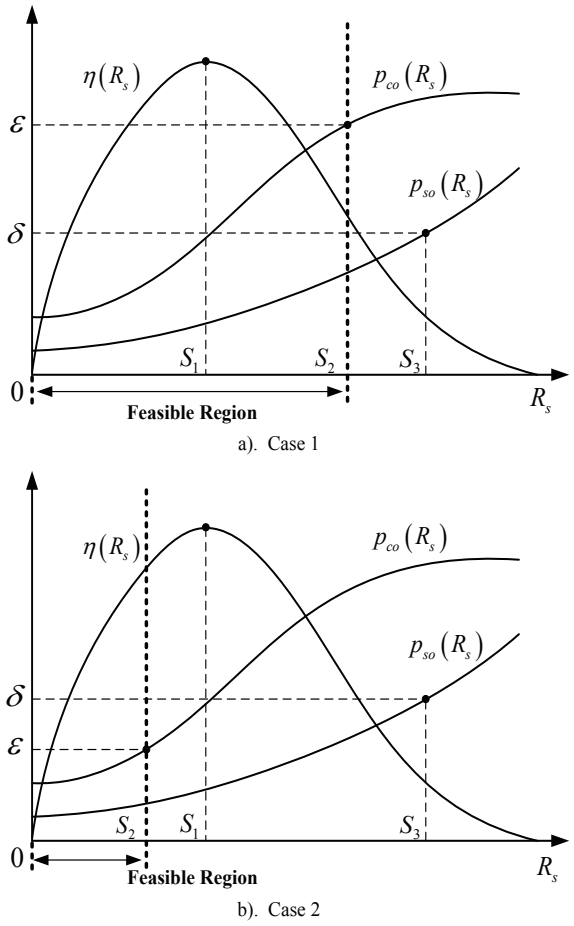


Fig. 6. Tho optimal $R_s$ maximizing the secrecy throughput with dual outage constraints.

***Proposition 1:*** The optimal $R_s$ that maximizes the secrecy throughput *in Scenario 1*, subject to the connection and secrecy constraints, is given by

$$R_{s_1}^* = \min\{S_1, S_2, S_3\}, \tag{44}$$

where $S_1$, $S_2$, and $S_3$ are given by (41), (42), and (43), respectively.

*Proof:* By solving (41), (42), and (43), the values of $S_1$, $S_2$, and $S_3$ can be obtained, as depicted in Fig. 6. For a given $\epsilon$ and $\delta$, the optimized $R_s$ must lie within not only the feasible region determined by $S_2$ but the feasible region determined by $S_3$. As such, the feasible region of $R_s$ is $\mathbb{S} = [0, \min\{S_2, S_3\}]$. Based on $\mathbb{S}$, we obtain the optimal $R_s$ maximizing the secrecy throughput with dual outage constraints in the following two cases:

- If $S_1 < \min\{S_2, S_3\}$, as depicted in Fig. 6a), $S_1$ lies within the feasible region $\mathbb{S}$. That is, the maximum $\eta_1(R_s)$ is still available in the feasible region $\mathbb{S}$, and $S_1$ is the unique solution. Hence, we have $R_{s_1}^* = S_1$. We highlight that in this case the outage constraints impose no effects on the optimal solution.
- If $S_1 \geq \min\{S_2, S_3\}$, as depicted in Fig. 6b), $S_1$ lies beyond the feasible region $\mathbb{S}$ and cannot be treated as the solution. Moreover, we find that $\eta_1(R_s)$ is a monotonous

increasing function of $R_s$ in the feasible region $\mathbb{S}$. As such, we take $R_{s_1}^* = \min\{S_2, S_3\}$ to guarantee that the highest secrecy throughput can be obtained.

To sum up the conclusions in the aforementioned two cases, the optimal $R_s$ maximizing the secrecy throughput with dual outage constraints in (44) can be obtained. ■

### B. Optimized $R_s$ for Scenario 2

In *Scenario 2*, the secrecy throughput is given by

$$\eta_2(R_s) = p_{tx_2}(R_s)\, p_{rst_2}(R_s)\, R_s. \tag{45}$$

Mathematically, we express $T_1$ as

$$T_1 = \underset{R_s}{\operatorname{argmax}} \quad \eta_2(R_s). \tag{46}$$

We first use the mathematical software package to take the first-order derivative of $\eta_2(R_s)$ with respect to $R_s$ and find that $\partial\eta_2(R_s)/\partial R_s$ is first positive and then negative. This indicates that there is a unique value of $R_s$ maximizing $\eta_2(R_s)$ subject to no outage constraints. Hence we conclude that (46) has a unique solution.

Based on the feasibility for the dual outage constraints presented in (37) and (39), we express $T_2$ and $T_3$ as

$$T_2 = \{R_s \,|p_{co_2}(R_s) = \epsilon\}, \tag{47}$$

and

$$\begin{aligned} T_3 &= \{R_s \,|p_{so_2}(R_s) = \delta\} \\ &= \begin{cases} \log_2\left(\frac{\delta\overline{\gamma}_b}{[\exp(-1)-\delta]\overline{\gamma}_e}\right), & \delta < \exp(-1) \\ \infty, & \delta \geq \exp(-1), \end{cases} \end{aligned} \tag{48}$$

respectively. As mentioned in Section III-B, $p_{co_2}(R_s)$ is a monotonous increasing function of $R_s$, which implies that (47) has a unique solution.

Despite that the closed-form solutions for $T_1$ and $T_2$ are mathematically intractable, we are still able to obtain them using a numerical method, e.g., bisection method. Based on above results, we present the optimal $R_s$ that meets (9) in *Scenario 2* in the following proposition.

***Proposition 2:*** The optimal $R_s$ that maximizes the secrecy throughput *in Scenario 2*, subject to two constraints, is given by

$$R_{s_2}^* = \min\{T_1, T_2, T_3\}, \tag{49}$$

where $T_1$, $T_2$, and $T_3$ are given by (46), (47), and (48) respectively.

*Proof:* The proof is similar with the proof for ***Proposition 1***. Here we omit the detailed proving process for brevity. ■

### C. Numerical Results

In this subsection, we present numerical results to investigate the impact of the dual outage constraints on the secrecy throughput in each scenario. Since our analytical results have been verified using Monte Carlo simulations in Section III-C, the Monte Carlo simulation points are omitted in this subsection to avoid unnecessarily cluttering.

Fig. 7 plots the secrecy throughput versus $R_s$ for two scenarios with different values of $\rho_b$ and $\rho_e$. In this figure, we

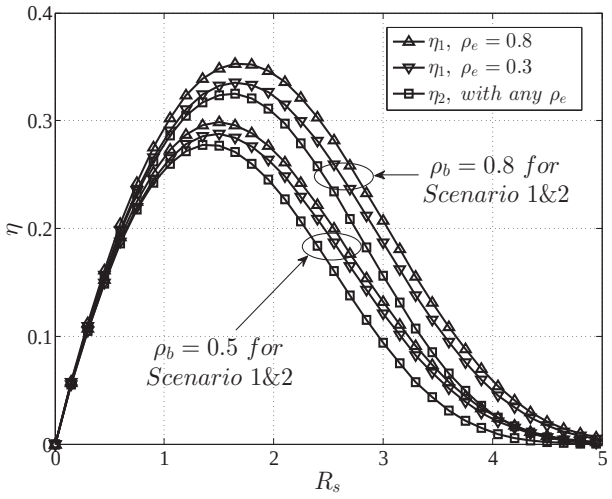


Fig. 7. Secrecy throughput subject to no outage constraints with outdated CSI for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

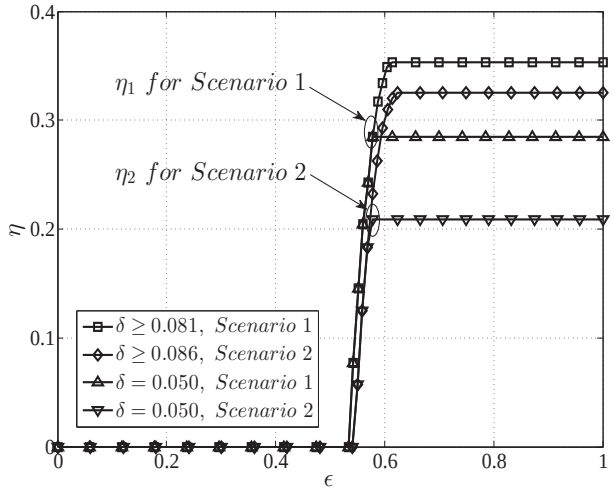


Fig. 8. Secrecy throughput versus reliability constraint with outdated CSI for $\rho_b = \rho_e = 0.8$, $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

generate $\eta_1(R_s)$ and $\eta_2(R_s)$ from (40) and (45), respectively. Moreover, we do not consider the reliability and security constraints such that $\epsilon = \delta = 1$. Moreover, we do not consider the reliability and security constraints such that $\epsilon = \delta = 1$. We first observe that the secrecy throughput first increases and then decreases as $R_s$ increases, indicating that an optimal $R_s$ indeed exists such that the secrecy throughput is maximized. Thus we clarify that (41) and (46) each have a unique solution. We also observe that the secrecy throughput decreases when $\rho_b$ or $\rho_e$ decreases. Furthermore, we observe that for the same $\rho_b$, the secrecy throughput in *Scenario 1* is higher than that in *Scenario 2*, even if $\rho_e$ is fairly low (e.g. $\rho_e = 0.3$). This is due to the fact that there is a higher probability to perform transmission in *Scenario 1* than that in *Scenario 2*. Thus *Scenario 1* offers a better secrecy throughput than *Scenario 2* without the outage constraints.

Fig. 8 and Fig. 9 plot the secrecy throughput for two

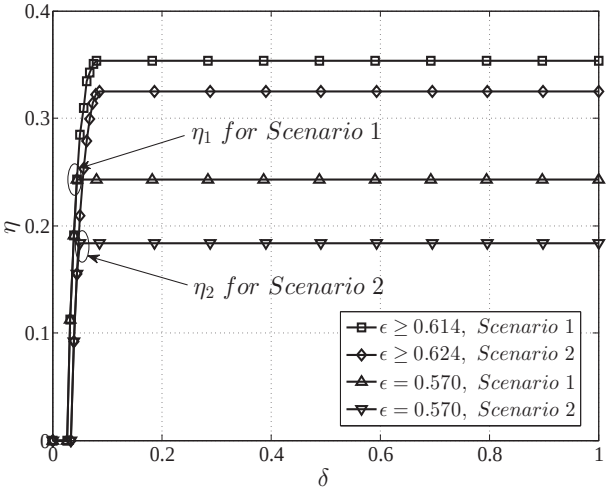


Fig. 9. Secrecy throughput versus security constraint with outdated CSI for $\rho_b = \rho_e = 0.8$, $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$dB.

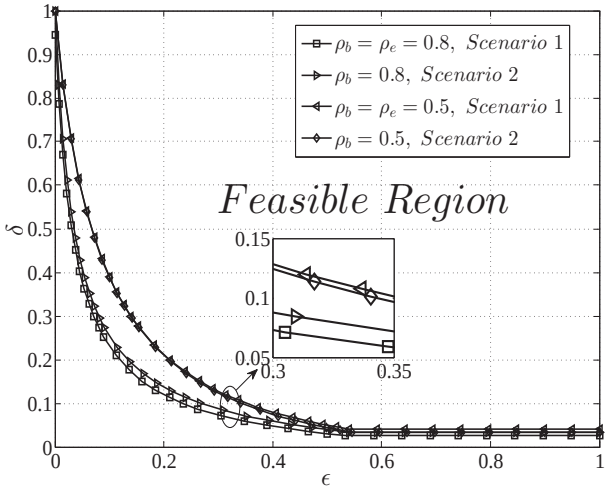


Fig. 10. Feasible security constraint versus feasible reliability constraint with outdated CSI for $\overline{\gamma}_b = 10$ dB and $\overline{\gamma}_e = 0$ dB.

scenarios versus the reliability constraint and the security constraint, respectively. We first observe that the secrecy throughput is a monotone non-decreasing function of either constraint. We then see that a positive secrecy throughput is achieved only when the two constraints are within the feasible ranges. For example, in Fig. 8 a positive secrecy throughput is achieved when $0.534 < \epsilon \leq 1$ in *Scenario 1* and when $0.541 < \epsilon \leq 1$ in *Scenario 2*. Moreover, in Fig. 9 a positive secrecy throughput is achieved when $0.027 < \delta \leq 1$ in *Scenario 1* and when $0.034 < \delta \leq 1$ in *Scenario 2*. Notably, we find that in the specifical case with $\rho_b = \rho_e = 0.8$, *Scenario 1* has a stricter security constraint and a stricter reliability constraint than *Scenario 2*. Furthermore, we observe that a constraint threshold exists such that the secrecy throughput keeps constant after the constraint exceeds the threshold. For example, it is seen from Fig. 8 and 9 that the maximum secrecy throughput in *Scenario 1* is achieved when $\epsilon \geq 0.614$ and $\delta \geq 0.081$, and the maximum secrecy throughput in *Scenario 2* is achieved when $\epsilon \geq 0.624$ and $\delta \geq 0.086$. This is due to the fact that the optimal $R_s$ can always be used to perform data transmission with the same secrecy throughput when the constraints are higher than the thresholds.

## V. Discussions

As seen in Section IV, $R_s$ is the only controllable parameter for transmission design. Our solutions of the optimal $R_s$ allow us to maximize the secrecy throughput subject to two constraints. We also note that the designed transmission schemes forgo the reliability level, as seen in Fig. 5. This is due to the fact that in the presence of the outdated CSI, the main channel quality known at Alice tends to be higher than the instantaneous channel capacity for secure transmission. As such, this transmission design may not be suitable for the systems where the reliability is in high demand. Motivated by this, in this section we present some discussions about the possible transmission design to improve reliability level.

Based on the aforementioned reasons, we believe that the use of $R_b = C_b$ makes the quality of the main channel to be overestimated. Thus it is wise for Alice to set $R_b$ as

$$R_b = \log_2\left(2^{R_s} + u\left(2^{C_b} - 2^{R_s}\right)\right), \tag{50}$$

where $u \in [0, 1]$. Note that when $u = 1$ we have $R_b = C_b$, and when $u = 0$ we have $R_b = R_s$. It is evident from (50) that the value of $R_b$ is within the feasible range of $[R_s, C_b]$.

By applying (50) into the system model in Section II-B and using the similar approaches in Section III, we can derive the closed-form expressions of $p_{co_1}(u, R_s)$, $p_{so_1}(u, R_s)$, $p_{co_2}(u, R_s)$ and $p_{so_2}(u, R_s)$. Thus the lower bounds on these outage probabilities for a given $u$, such as $p_{co_1,LB}(u)$, $p_{so_1,LB}(u)$, $p_{co_2,LB}(u)$ and $p_{so_2,LB}(u)$, can be obtained by setting $R_s = 0$. Here the detailed derivations are omitted for brevity. We then find that the choice of $R_b$, indicated by (50), enables a trade-off between the feasible reliability constraint and the feasible security constraint. For example, a lower $R_b$ leads to a lower connection outage probability but a higher secrecy outage probability. This implies that if we set a looser reliability constraint, the security constraint becomes stricter.

To illustrate this trade-off between the feasible reliability constraint and the feasible security constraint, Fig. 10 plots the new feasible region of the dual outage constraints for both scenarios. In this figure, the curves are generated by using the values of $p_{co_1,LB}(u)$, $p_{so_1,LB}(u)$, $p_{co_2,LB}(u)$ and $p_{so_2,LB}(u)$ at all values of $u$. For each scenario with fixed $\rho_b$ and $\rho_e$, the feasible region of $\epsilon$ and $\delta$ lies in the region above the corresponding curve. We first observe that when $u$ increases, the lower bound on the connection outage probability increases, but the lower bound on the secrecy outage probability decreases. For example, in *Scenario 2* when $u$ increases from 0 to 1, the lower bound on the connection outage probability increases from 0 to $p_{co_2,LB}$, as indicated by (36), while the lower bound on the secrecy outage probability decreases from 1 to $p_{so_2,LB}$, as indicated by (38). This observation is not surprising since allowing more freedom

on $R_b$ enables a trade-off between reliability and security. Notably, this trade-off leads to a profound extension in the feasible region compared with Fig. 5. We also observe the extension of the feasible region when $\rho_b$ or $\rho_e$ increases, which is due to that the uncertainty in the main channel and the eavesdropper's channel decreases when $\rho_b$ and $\rho_e$ increase, respectively. This indicates that the more knowledge about the channel quality is known at Alice, the better reliability and security levels can be achieved.

## VI. Conclusion

In the presence of outdated CSI, we adopted the on-off scheme to help perform secure transmission, under which we conducted the secrecy performance in wiretap channel and then presented the design of wiretap coding parameters. In particular, we considered the two scenarios with different assumptions on the CSI from the eavesdropper. For each scenario, we derived the transmission probability, the connection outage probability, the secrecy outage probability as well as the reliable and secure transmission probability. Based on these results, we determined the optimal secrecy rates that maximize the secrecy throughput under dual connection and secrecy outage constraints. Moreover, we found that a larger feasible region of the dual outage constraints can be obtained by optimizing the codeword transmission rate.

## Appendix A
## Derivation of $p_{co_1}(R_s)$ in (12)

Based on (11), we formulate $p_{co_1}(R_s)$ as

$$\begin{aligned} p_{co_1}(R_s) &= \Pr\left\{\tilde{C}_b < C_b \,|C_b - C_e \geq R_s\right\} \\ &= \Pr\left\{\tilde{\gamma}_b < \gamma_b \,\middle|\gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\} \\ &= \frac{\Pr\left\{\tilde{\gamma}_b < \gamma_b, \gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\}}{\Pr\left\{\gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\}}. \end{aligned} \tag{51}$$

We first re-express the numerator of $p_{co_1}(R_s)$ as

$$\begin{aligned} &\Pr\left\{\tilde{\gamma}_b < \gamma_b, \gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\} \\ &= \underbrace{\int_0^{\infty} \int_{2^{R_s}(1+x)-1}^{\infty} \underbrace{\int_0^{y} f_{\tilde{\gamma}_b|\gamma_b}(z\,|y)\,dz}_{\Xi_1} f_{\gamma_b}(y)\,dy f_{\gamma_e}(x)\,dx}_{\Xi_2}. \end{aligned} \tag{52}$$

Recall that $\tilde{\gamma}_b$ and $\gamma_b$ are two correlated exponential random variables (RVs). The conditional PDF of $\tilde{\gamma}_b$ conditioned on a given $\gamma_b$ is given by

$$\begin{aligned} f_{\tilde{\gamma}_b|\gamma_b}(z\,|y) =& \frac{1}{(1-\rho_b^2)\,\bar{\gamma}_b} \exp\left(-\frac{z+\rho_b^2 y}{(1-\rho_b^2)\,\bar{\gamma}_b}\right) \\ &\times I_0\left(\frac{2\rho_b\sqrt{zy}}{(1-\rho_b^2)\,\bar{\gamma}_b}\right). \end{aligned} \tag{53}$$

Substituting (53) into $\Xi_1$, we derive $\Xi_1$ as

$$\Xi_1 = 1 - Q_1\left(\sqrt{\frac{2\rho_b^2 y}{(1-\rho_b^2)\,\bar{\gamma}_b}}, \sqrt{\frac{2y}{(1-\rho_b^2)\,\bar{\gamma}_b}}\right), \tag{54}$$

where $Q_1(a,b)$ represents the Marcum's Q-function [34]. We then use the series representation of Marcum's Q-function in terms of Bessel functions, given by

$$Q_1(a,b) = \exp\left(-\frac{a^2+b^2}{2}\right) \sum_{n=0}^{\infty} \left(\frac{a}{b}\right)^n I_n(ab), \tag{55}$$

and the expansion of Bessel function [33, Eq. (8.445)], given by

$$I_v(z) = \sum_{k=0}^{\infty} \frac{1}{k!\Gamma(v+k+1)} \left(\frac{z}{2}\right)^{v+2k}, \tag{56}$$

to obtain the series representation of $\Xi_1$, which yields

$$\begin{aligned} \Xi_1 =& 1 - \exp\left(-\frac{\left(1+\rho_b^2\right)y}{\left(1-\rho_b^2\right)\bar{\gamma}_b}\right) \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\rho_b^{2(n+k)}}{k!} \\ &\times \frac{1}{\Gamma(n+k+1)} \left(\frac{y}{(1-\rho_b^2)\,\bar{\gamma}_b}\right)^{n+2k}. \end{aligned} \tag{57}$$

Substituting (57) into $\Xi_2$, we derive $\Xi_2$ as

$$\begin{aligned} \Xi_2 =& \exp\left(-\frac{2^{R_s}x + 2^{R_s} - 1}{\bar{\gamma}_b}\right) - \exp\left(-\frac{2\left(2^{R_s}-1\right)}{(1-\rho_b^2)\,\bar{\gamma}_b}\right) \\ &\times \exp\left(-\frac{2^{1+R_s}x}{(1-\rho_b^2)\,\bar{\gamma}_b}\right) \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\rho_b^{2(n+k)}\left(1-\rho_b^2\right)}{k!2^{n+2k+1}} \\ &\times \frac{(n+2k)!}{(n+k)!} \sum_{m=0}^{n+2k}\sum_{q=0}^{m} \frac{\left(2^{R_s}-1\right)^{m-q} 2^{m+qR_s} x^q}{q!\,(m-q)!((1-\rho_b^2)\,\bar{\gamma}_b)^m}. \end{aligned} \tag{58}$$

Substituting (58) into (52) and solve the resultant integrals, the numerator of $p_{co_1}(R_s)$ is obtained. We also note that the denominator of $p_{co_1}(R_s)$ is given by (10). Therefore, we obtain $p_{co_1}(R_s)$ in (12).

## Appendix B
## Derivation of $p_{so_1}(R_s)$ in (14)

Based on (13), we formulate $p_{so_1}(R_s)$ as

$$\begin{aligned} p_{so_1}(R_s) &= \Pr\left\{C_b - R_s < \tilde{C}_e \,|C_b - C_e \geq R_s\right\} \\ &= \Pr\left\{\gamma_b < 2^{R_s}(1+\tilde{\gamma}_e) - 1 \,\middle|\gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\} \\ &= \frac{\Pr\left\{\gamma_b < 2^{R_s}(1+\tilde{\gamma}_e) - 1, \gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\}}{\Pr\left\{\gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\}}. \end{aligned} \tag{59}$$

We re-express the numerator of $p_{so_1}(R_s)$ as

$$\begin{aligned} &\Pr\left\{\gamma_b < 2^{R_s}(1+\tilde{\gamma}_e) - 1, \gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\} \\ &= \Pr\left\{\tilde{\gamma}_e > 2^{-R_s}(1+\gamma_b) - 1, \gamma_e \leq 2^{-R_s}(1+\gamma_b) - 1\right\} \\ &= \int_{2^{R_s}-1}^{\infty} \underbrace{\int_0^{2^{-R_s}(1+x)-1} \Phi_1 f_{\gamma_e}(y)\,dy}_{\Phi_2} f_{\gamma_b}(x)\,dx, \end{aligned} \tag{60}$$

where $\Phi_1$ is

$$\Phi_1 = \int_{2^{-R_s}(1+x)-1}^{\infty} f_{\tilde{\gamma}_e|\gamma_e}(z\,|y)\,dz. \tag{61}$$

Recall that $\tilde{\gamma}_e$ and $\gamma_e$ are two correlated exponential RVs. The conditional PDF of $\tilde{\gamma}_e$ conditioned on a given $\gamma_e$ is given by

$$f_{\tilde{\gamma}_e|\gamma_e}(z|y) = \frac{1}{(1-\rho_e^2)\bar{\gamma}_e} \exp\left(-\frac{z+\rho_e^2 y}{(1-\rho_e^2)\bar{\gamma}_e}\right) \times I_0\left(\frac{2\rho_e\sqrt{zy}}{(1-\rho_e^2)\bar{\gamma}_e}\right). \quad (62)$$

We then substitute (62) into (61) to derive $\Phi_1$ as

$$\Phi_1 = Q_1\left(\sqrt{\frac{2\rho_e^2 y}{(1-\rho_e^2)\bar{\gamma}_e}}, \sqrt{\frac{2^{1-R_s}(x+1)-2}{(1-\rho_e^2)\bar{\gamma}_e}}\right). \quad (63)$$

With the help of (55) and (56), the series representation of $\Phi_1$ is obtained as

$$\Phi_1 = \exp\left(-\frac{\rho_e^2 y + 2^{-R_s}x + 2^{-R_s} - 1}{(1-\rho_e^2)\bar{\gamma}_e}\right) \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{1}{k!} \times \frac{\rho_e^{2(n+k)} y^{n+k}\left(2^{-R_s}x + 2^{-R_s} - 1\right)^k}{\Gamma(n+k+1)\left((1-\rho_e^2)\bar{\gamma}_e\right)^{n+2k}}. \quad (64)$$

Substituting (64) into $\Phi_2$, we obtain the series representation of $\Phi_2$ as

$$\Phi_2 = \exp\left(-\frac{x+1-2^{R_s}}{(1-\rho_e^2)2^{R_s}\bar{\gamma}_e}\right) \sum_{n=0}^{\infty}\sum_{k=0}^{\infty} \frac{\rho_e^{2(n+k)}\left(1-\rho_e^2\right)}{k!\left((1-\rho_e^2)\bar{\gamma}_e\right)^k} \times \left(\frac{x+1-2^{R_s}}{2^{R_s}}\right)^k \left[1 - \exp\left(-\frac{x+1-2^{R_s}}{(1-\rho_e^2)2^{R_s}\bar{\gamma}_e}\right) \times \sum_{m=0}^{n+k} \frac{1}{m!}\left(\frac{x+1-2^{R_s}}{(1-\rho_e^2)2^{R_s}\bar{\gamma}_e}\right)^m\right]. \quad (65)$$

Finally, we substitute (65) into (60) and solve the resultant integrals to obtain numerator of $p_{so_1}(R_s)$. Hence, $p_{so_1}(R_s)$ in (14) can be obtained.

## APPENDIX C
## DERIVATION OF $p_{rst_1}(R_s)$ IN (18)

Based on (17), we formulate $p_{rst_1}(R_s)$ as

$$\begin{aligned} p_{rst_1}(R_s) &= \Pr\left\{\tilde{C}_b \geq C_b, C_b - R_s \geq \tilde{C}_e \,|C_b - C_e \geq R_s\right\} \\ &= \Pr\left\{\tilde{\gamma}_b \geq \gamma_b, \gamma_b \geq 2^{R_s}(1+\tilde{\gamma}_e) - 1 \,\middle|\, \gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\} \\ &= \frac{\Pr\left\{\tilde{\gamma}_b \geq \gamma_b, \gamma_b \geq 2^{R_s}(1+\tilde{\gamma}_e) - 1, \gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\}}{\Pr\left\{\gamma_b \geq 2^{R_s}(1+\gamma_e) - 1\right\}}. \end{aligned} \quad (66)$$

By re-expressing the numerator of $p_{rst_1}(R_s)$ we obtain

$$\Pr\left\{\tilde{\gamma}_b \geq \gamma_b, \tilde{\gamma}_e \leq \frac{1+\gamma_b}{2^{R_s}} - 1, \gamma_e \leq \frac{1+\gamma_b}{2^{R_s}} - 1\right\} = \int_{2^{R_s}-1}^{\infty} \Delta_1 \Delta_2 f_{\gamma_b}(x)\, dx, \quad (67)$$

where $\Delta_1$ is

$$\Delta_1 = \Pr\left\{\tilde{\gamma}_b \geq x\right\} = \int_x^{\infty} f_{\tilde{\gamma}_b|\gamma_b}(w|x)\, dw, \quad (68)$$

and $\Delta_2$ is

$$\begin{aligned} \Delta_2 &= \Pr\left\{\tilde{\gamma}_e \leq 2^{-R_s}(1+x) - 1, \gamma_e \leq 2^{-R_s}(1+x) - 1\right\} \\ &= \int_0^{2^{-R_s}(1+x)-1} \int_0^{2^{-R_s}(1+x)-1} f_{\tilde{\gamma}_e|\gamma_e}(z|y)\, dz f_{\gamma_e}(y)\, dy. \end{aligned} \quad (69)$$

With the help of $\Xi_1$ in Appendix A and $\Phi_2$ in Appendix B, we obtain the series representations of $\Delta_1$ and $\Delta_2$ as

$$\Delta_1 = 1 - \Xi_1 \quad (70)$$

and

$$\Delta_2 = 1 - \exp\left(-\frac{2^{-R_s}x + 2^{-R_s} - 1}{\bar{\gamma}_e}\right) - \Phi_2, \quad (71)$$

where $\Xi_1$ is given by (57) and $\Phi_2$ is given by (65).

Finally, we substitute (70) and (71) into (67) and solve the resultant integrals, the numerator of $p_{rst_1}(R_s)$ is obtained. Using (10), $p_{rst_1}(R_s)$ in (18) can be obtained.

## REFERENCES


[1] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[2] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

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

[4] 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.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Techn. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

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

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

[9] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, June 2012.

[10] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[11] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.

[12] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[13] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics Security*, accepted to appear.

[14] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[15] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[16] J. M. Taylor, M. Hempel, H. Sharif, S. Ma, and Y. Yang, "Impact of channel estimation errors on effectiveness of eigenvector-based jamming for physical layer security in wireless networks," in *Proc. IEEE CAMAD Workshop*, Kyoto, Japan, June 2011, pp. 122–126.

[17] T. Y. Liu, S. C. Lin, T. H. Chang, and Y. W. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, June 2012, pp. 4782–4787.

[18] M. Pei, J. Wei, K. K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[19] 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.

[20] S. Bashar, Z. Ding, and Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[21] S. C. Lin, T. H. Chang, Y. L. Liang, Y. W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[22] L. Sun and S. Jin, "On the ergodic secrecy rate of multiple-antenna wiretap channels using artificial noise and finite-rate feedback," in *Proc. IEEE Int. Symp. Personal Indoor Mobile Radio Commun.*, Toronto, Canada, Sep. 2011, pp. 1–5.

[23] Z. Rezki, A. Khisti, and M. S. Alouini, "On the ergodic secret message capacity of the wiretap channel with finite-rate feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, America, Jul. 2012, pp. 239–243.

[24] 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.

[25] 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.

[26] N. S. Ferdinand, D. B. Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection", *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, May 2013.

[27] 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.

[28] 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.

[29] 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.

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

[31] A. Khisti and G. Wornell, "Secure transmission with multiple antennas – Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[32] 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.

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

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