Impact of Channel Estimation Error on Secure Transmission Design

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

***Abstract*—In this paper, we investigate the secure transmission design with practical assumptions on the channel state information (CSI). Specifically, the CSI of the legitimate link is imperfectly estimated and the CSI of the eavesdropper is unknown to the legitimate users. We derive both a fixed-rate and an adaptive-rate transmission schemes by explicitly considering the rate parameters of the wiretap code in the secure transmission design. The derived schemes achieve the maximum throughput subject to constraints on the secrecy performance against eavesdropping and the reliability performance against channel estimation error. For a given target throughput requirement, our numerical results illustrate how the security performance needs to be compromised when the accuracy of channel estimation reduces. One interesting finding is that the security cost of having a small amount of channel estimation error is low, while the security cost increases fast when the channel estimation error becomes considerable.**

I. Introduction

The broadcast nature of wireless networks makes communication security a critical issue, especially when the information transmitted is important and private. Cryptographic technologies are traditionally used to increase the wireless communication security. On the other hand, information-theoretical physical layer security has been widely regarded as a complement to cryptographic technologies in future networks. Wyner's pioneering work introduced the wiretap channel model as a framework for information-theoretic security [1]. The model of broadcast channels with confidential messages was described by Csiszár and Körner in [2]. In recent years, considerable work has been done in this area by taking the properties of wireless fading channels into account, with increasing attention paid to a more practical scenario where the eavesdropper's instantaneous channel state information (CSI) is unknown at the transmitter.

However, one of the main assumptions in most of the previous work is that the CSI of the legitimate link is perfectly known at both the legitimate receiver and the transmitter. Since obtaining the CSI of the legitimate link is a channel estimation problem which generally is not error-free, the assumption of perfectly knowing CSI is impractical. Therefore, it is worthwhile investigating the impact of the legitimate receiver's channel estimation error on the secure transmission. Initial works that considered imperfect CSI of the legitimate receiver and no CSI of the eavesdropper can be found in [3–5].

In [3], Taylor et al. presented the impact of the legitimate receiver's channel estimation error on the performance of an eigenvector based jamming technique. Their research showed that the secrecy capacity provided by the jamming technique decreases rapidly as the channel estimation error increases. Zhou and Mckay analyzed the optimal power allocation of the artificial noise for the secure transmission considering the impact of imperfect CSI of the legitimate receiver in [4]. They found that, when the CSI is imperfectly obtained, it is wise to create more artificial noise by compromising on the transmit power of information-bearing signals. In [5], Mukherjee and Swindlehurst pointed out that the security provided by beamforming approaches is quite sensitive to the imprecise channel estimates. They also proposed a robust beamforming scheme for the multiple-input multiple-output (MIMO) secure transmission system with imperfect CSI of the legitimate receiver.

Although the aforementioned works have performed some analyses on the impact of the legitimate receiver's channel uncertainty, none of them considered the rate parameters of secure transmission as part of the system design. While, in this paper, we explicitly investigate the optimal choices of the confidential information rate and the codeword transmission rate, which are the important rate parameters of a wiretap code. Under the practical assumptions that the legitimate receiver's instantaneous CSI is imperfectly estimated and the eavesdropper's instantaneous CSI is unknown at the transmitter, we design two secure transmission schemes, each of which maximizes the throughput while satisfying a certain level of security and reliability requirements. The first scheme is designed for fixed-rate transmission and it requires only one-bit feedback from the legitimate receiver to avoid unnecessary transmission when the legitimated link is in deep fade. The second scheme is designed for adaptive-rate transmission and it requires the feedback of the instantaneous estimated CSI. Our numerical results demonstrate how the channel estimation error affects the maximum achievable throughput or the security performance for a given throughput. The trade-off between security against eavesdropping and reliability against channel estimation error is also discussed.

II. System Model

We consider a wireless communication system in which the transmitter, Alice, wants to send confidential information to the legitimate receiver, Bob, over a slow Rayleigh fading channel in the presence of an eavesdropper, Eve. Each of Alice, Bob and Eve has a single antenna. The received symbols at Bob

978-1-4673-4675-7/13/$31.00 ©2013 IEEE

and Eve are, respectively, given by

$$y_b = \sqrt{P_b} h_b x + n_b, \tag{1}$$

$$y_e = \sqrt{P_e} h_e x + n_e, \tag{2}$$

in which h_b and h_e denote the channel gains from Alice to Bob and Eve, respectively, both with complex Gaussian distribution $\mathcal{CN}(0,1)$. The additive white noise with complex Gaussian distribution $\mathcal{CN}(0,1)$ at Bob and Eve are denoted by n_b and n_e. The transmitted signals are normalized so that $E\left(|x|^2\right) = 1$, where $E(\cdot)$ is the expectation operation. Thus, P_b and P_e represent the average signal-to-noise ratios (SNRs) at Bob and Eve without the consideration of channel uncertainty. Bob knows his instantaneous CSI imperfectly and an error-free feedback link exists from Bob to Alice. To establish a worst case scenario analysis, we assume that Eve knows her instantaneous CSI perfectly. The instantaneous SNR at Eve is $\gamma_e = P_e|h_e|^2$, which has an exponential distribution given by

$$f_{\gamma_e}(\gamma_e) = \frac{1}{\bar{\gamma}_e} \exp\left(-\frac{\gamma_e}{\bar{\gamma}_e}\right), \quad \gamma_e > 0, \tag{3}$$

where $\bar{\gamma}_e$ is the average SNR at Eve.

We assume that Alice knows the statistics of both Bob and Eve's channels. Different assumptions on the feedback information from Bob to Alice are considered, as discussed later in Section III. However, Alice does not know Eve's instantaneous CSI, and therefore, achieving the perfect secrecy is not always possible.

A. Channel Estimation

We assume that Bob's channel is estimated by an MMSE estimator. The estimation of Bob's channel coefficient and the estimation error are denoted by $\hat{h}_b$ and $\tilde{h}_b$, respectively. Thus,

$$h_b = \hat{h}_b + \tilde{h}_b, \tag{4}$$

where $\hat{h}_b$ and $\tilde{h}_b$ have zero-mean complex Gaussian distributions. In fact, $P|\hat{h}_b|^2$ is what Bob would feed back to Alice as the estimated instantaneous SNR. The orthogonality principle implies $E(|h_b|^2) = E(|\hat{h}_b|^2) + E(|\tilde{h}_b|^2)$. We further assume that the variance of the estimation error, $\beta = E(|\tilde{h}_b|^2)$, is known at both Bob and Alice. For convenience, we let $\hat{\gamma}_b = P_b|\hat{h}_b|^2$ and $\tilde{\gamma}_b = P_b|\tilde{h}_b|^2$, each having an exponential distribution given by

$$f_{\hat{\gamma}_b}(\hat{\gamma}_b) = \frac{1}{\bar{\hat{\gamma}}_b} \exp\left(-\frac{\hat{\gamma}_b}{\bar{\hat{\gamma}}_b}\right), \quad \hat{\gamma}_b > 0, \tag{5}$$

$$f_{\tilde{\gamma}_b}(\tilde{\gamma}_b) = \frac{1}{\bar{\tilde{\gamma}}_b} \exp\left(-\frac{\tilde{\gamma}_b}{\bar{\tilde{\gamma}}_b}\right), \quad \tilde{\gamma}_b > 0, \tag{6}$$

where $\bar{\hat{\gamma}}_b$ and $\bar{\tilde{\gamma}}_b$ are the mean values of $\hat{\gamma}_b$ and $\tilde{\gamma}_b$. Then, the actual instantaneous SNR at Bob can be written as [6]

$$\gamma_b = \frac{P_b|\hat{h}_b|^2}{P_b|\tilde{h}_b|^2 + 1} = \frac{\hat{\gamma}_b}{\tilde{\gamma}_b + 1}. \tag{7}$$

B. Secure Encoding

We consider the widely-adopted wiretap code [1]. There are two rate parameters chosen by the encoder, namely, the codeword transmission rate, R_b, and the confidential information rate, R_s. The positive rate difference $R_e = R_b - R_s$ is the cost to provide secrecy against the eavesdropper. A length M wiretap code is constructed by generating 2^{MR_b} codewords $x^M(w,v)$ of length M, where $w = 1, 2, \cdots, 2^{MR_s}$ and $v = 1, 2, \cdots, 2^{M(R_b - R_s)}$. For each message index w, we randomly select v from $\left\{1, 2, \cdots, 2^{M(R_b-R_s)}\right\}$ with uniform probability and transmit the codeword $x^M(w,v)$. From [1, 7], perfect secrecy cannot be achieved when $R_e < C_e$, where C_e denotes Eve's channel capacity, $C_e = \log_2(1+\gamma_e)$. Also, Bob is unable to decode the received codewords correctly when $R_b > C_b$, where C_b denotes Bob's channel capacity, $C_b = \log_2(1+\gamma_b)$. Thus, given a pair of the rate choices, R_b and R_s, we define the secrecy outage probability [8], p_{so}, and the connection outage probability, p_{co}, as

$$p_{so} = \Pr(C_e > R_b - R_s), \tag{8}$$

$$p_{co} = \Pr(C_b < R_b), \tag{9}$$

where $\Pr(\cdot)$ denotes the probability measure. The security level and the reliability level of a transmission scheme can then be measured by the secrecy outage probability and the connection outage probability, respectively.

III. Transmission Design

In this section, two on-off secure transmission schemes are designed. Similar transmission schemes without the consideration of channel estimation error was studied in [9]. Alice decides whether or not to transmit according to the information about Bob's estimated instantaneous SNR, i.e., transmission takes place when the estimated instantaneous SNR, $\hat{\gamma}_b$, is greater than an SNR threshold, μ, and transmission is suspended when $\hat{\gamma}_b$ is less than μ. Having this on-off scheme is worthwhile and important, because it would significantly reduce the secrecy outage probability, which can be seen later.

We consider the design problem of maximizing the system throughput, η, subject to two constraints, one on the security performance and the other on the reliability performance. The design problem can be written as

$$\max \qquad \eta, \qquad \text{s.t.} \;\; p_{so} \le \epsilon, p_{co} \le \delta, \tag{10}$$

where $\epsilon \in [0,1]$ and $\delta \in [0,1]$ represent the minimum security and reliability requirements. The controllable parameters to design are the codeword transmission rate, R_b, the confidential information rate, R_s, and the on-off SNR threshold, μ. In what follows, two different transmission schemes are designed, according to whether Alice has limited or full knowledge of Bob's estimated instantaneous CSI. The expression of the system throughput for each transmission scheme is provided in the corresponding subsection.

A. Fixed-Rate Transmission Scheme

First, we consider the scenario where the codeword transmission rate, R_b, and the confidential information rate, R_s, are both fixed over time. This design requires only one-bit feedback to enable the on-off transmission. Since the confidential information rate is fixed, the system throughput for the fixed-rate transmission scheme is given by

$$\eta = p_{tx}(1-p_{co})R_s, \tag{11}$$

where p_{tx} denotes the probability of transmission. The on-off transmission scheme works as mentioned previously, i.e., transmission takes place when $\hat{\gamma}_b > \mu$ and transmission is suspended when $\hat{\gamma}_b \leq \mu$. For any chosen values of R_b, R_s, and μ, the transmission probability is given by

$$p_{tx}(\mu) = \Pr(\hat{\gamma}_b > \mu) = \exp(-\mu/\bar{\tilde{\gamma}}_b) \tag{12}$$

and the secrecy outage probability can be computed as

$$\begin{aligned} p_{so}(R_b, R_s) &= \Pr(C_e > R_b - R_s) \\ &= \exp\left(-\frac{2^{R_b-R_s}-1}{\bar{\gamma}_e}\right). \end{aligned} \tag{13}$$

Since $\hat{\gamma}_b \geq \gamma_b$ (as given in (7)) and transmission should not take place when $C_b < R_b$, it is wise to choose μ that satisfies

$$\log_2(1+\mu) \geq C_b \geq R_b \Rightarrow \mu \geq 2^{R_b} - 1. \tag{14}$$

Also, since message transmission takes place only when $\hat{\gamma}_b > \mu$, the connection outage probability is given by[1]

$$\begin{aligned} p_{co}(\mu, R_b) &= \Pr\left(\log_2(1+\gamma_b) < R_b | \hat{\gamma}_b > \mu\right) \\ &= \Pr\left(\log_2\left(1+\frac{\hat{\gamma}_b}{\tilde{\gamma}_b+1}\right) < R_b | \hat{\gamma}_b > \mu\right) \\ &= \frac{\Pr(\mu < \hat{\gamma}_b < (2^{R_b}-1)(\tilde{\gamma}_b+1))}{\Pr(\hat{\gamma}_b > \mu)} \\ &= \exp\left(\frac{\mu}{\bar{\tilde{\gamma}}_b}\right) \\ &\quad \cdot \int_{\frac{\mu}{2^{R_b}-1}-1}^{\infty} \left(\int_{\mu}^{(2^{R_b}-1)(\tilde{\gamma}_b+1)} f_{\hat{\gamma}_b}(\hat{\gamma}_b) \mathrm{d}\hat{\gamma}_b \right) f_{\tilde{\gamma}_b}(\tilde{\gamma}_b) \mathrm{d}\tilde{\gamma}_b \\ &= \frac{\bar{\tilde{\gamma}}_b(2^{R_b}-1)}{\bar{\tilde{\gamma}}_b(2^{R_b}-1)+\bar{\tilde{\gamma}}_b} \exp\left(\frac{1}{\bar{\tilde{\gamma}}_b}\left(1-\frac{\mu}{2^{R_b}-1}\right)\right). \end{aligned} \tag{15}$$

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

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

The following proposition summarizes the solution to the design problem for the fixed-rate transmission scheme, where each of the optimal μ and the optimal R_s is expressed as a closed-form function of R_b and the optimal R_b is obtained by numerically solving an optimization problem.

Proposition 1: The optimal parameters of the fixed-rate transmission scheme are given as follow:

$$\mu = \begin{cases} 2^{R_b}-1, & \text{if } R_b \leq \log_2\left(1+\frac{\bar{\tilde{\gamma}}_b\delta}{\bar{\tilde{\gamma}}_b(1-\delta)}\right), \\ \left(2^{R_b}-1\right)\left(1-\bar{\tilde{\gamma}}_b \ln\left(\delta\frac{\bar{\tilde{\gamma}}_b(2^{R_b}-1)+\bar{\tilde{\gamma}}_b}{\bar{\tilde{\gamma}}_b(2^{R_b}-1)}\right)\right), & \text{otherwise.} \end{cases} \tag{16}$$

$$R_s = R_b - k, \qquad \text{where} \quad k = \log_2(1+\bar{\gamma}_e \ln \epsilon^{-1}). \tag{17}$$

R_b is obtained by solving the problem given as

$$\begin{aligned} \arg\max_{R_b} \quad & (R_b-k)\exp\left(-\frac{\mu}{\bar{\tilde{\gamma}}_b}\right) \\ & \cdot\left(1-\frac{\bar{\tilde{\gamma}}_b\left(2^{R_b}-1\right)}{\bar{\tilde{\gamma}}_b\left(2^{R_b}-1\right)+\bar{\tilde{\gamma}}_b}\exp\left(\frac{1}{\bar{\tilde{\gamma}}_b}\left(1-\frac{\mu}{2^{R_b}-1}\right)\right)\right), \\ \text{s.t.} \quad & k<R_b<\max\left\{\log_2\left(1+\frac{\bar{\tilde{\gamma}}_b\delta}{\bar{\tilde{\gamma}}_b(1-\delta)}\right), k+\frac{1}{\ln 2}W\left(2^{-k}\bar{\tilde{\gamma}}_b\right)\right\}, \end{aligned}$$

where $W(\cdot)$ is the Lambert W function and μ is a function of R_b whose expression is formulated as (16).

Proof: We first prove the expressions for the optimal R_s and the optimal μ for any chosen R_b as follow. Since $p_{tx}(\mu)$ in (12) and $p_{co}(\mu, R_b)$ in (15) are independent of R_s, it is optimal to maximize R_s. Hence, we obtain the optimal R_s while satisfying $p_{so}(R_b, R_s) \leq \epsilon$ as (17). Then, the optimization problem can be rewritten as

$$\begin{aligned} \arg\max_{\mu, R_b} \quad & G(\mu, R_b) = p_{tx}(\mu)\left(1-p_{co}(\mu, R_b)\right)(R_b-k), \\ \text{s.t.} \quad & p_{co}(\mu, R_b) \leq \delta, \mu \geq 2^{R_b}-1, R_b - k > 0. \end{aligned}$$

To satisfy the reliability constraint, $p_{co}(\mu, R_b) \leq \delta$, we have

$$\mu \geq \left(2^{R_b}-1\right)\left(1-\bar{\tilde{\gamma}}_b \ln\left(\delta\frac{\bar{\tilde{\gamma}}_b(2^{R_b}-1)+\bar{\tilde{\gamma}}_b}{\bar{\tilde{\gamma}}_b(2^{R_b}-1)}\right)\right). \tag{18}$$

For any given value of R_b, $\mu = 2^{R_b}-1$ is the only solution of μ to the equation

$$\frac{\partial G(\mu, R_b)}{\partial \mu} = 0 \tag{19}$$

and $\frac{\partial^2 G(2^{R_b}-1, R_b)}{\partial \mu^2} < 0$. Thus, if we ignore the possible lower bound of μ given by (18), the optimal μ is equal to $2^{R_b}-1$. Then, considering the lower bound, the optimal μ is formulated as (16). It is easy to prove that when

$$R_b \geq \max\left\{\log_2\left(1+\frac{\bar{\tilde{\gamma}}_b\delta}{\bar{\tilde{\gamma}}_b(1-\delta)}\right), k+\frac{1}{\ln 2}\mathrm{W}\left(2^{-k}\bar{\tilde{\gamma}}_b\right)\right\},$$

$$\frac{\partial G(\mu, R_b)}{\partial R_b} < 0. \tag{20}$$

Thus, the optimal R_b can be obtained by solving the optimization problem given in Proposition 1. ■

Remark: Apart from solving the optimization problem, it is important to know the condition under which the security and reliability constraints are feasible. Here, the feasibility of constraints means that the constraints can be satisfied whilst

[1]The connection outage probability here is a conditional probability which explicitly takes into account the condition under which transmission takes place due to the on-off scheme. This is different from the basic expression in (9) which implicitly assumes that transmission has happened. Indeed, the secrecy outage probability in (13) also has the conditioning of $\hat{\gamma}_b > \mu$. But this condition is independent of C_e, hence is simply removed.

achieving a positive confidential information rate. To satisfy $R_s > 0$ and $p_{so}(R_b, R_s) \leq \epsilon$, we have $2^{R_b} - 1 > \bar{\gamma}_e \ln \epsilon^{-1}$. Also, from (14) and (18), we have $2^{R_b} - 1 \leq \min\{\mu, F(\mu, \delta)\}$ where $F(\mu, \delta)$ is the positive solution of x to the equation

$$\mu = x\left(1 - \bar{\bar{\gamma}}_b \ln\left(\delta \frac{\bar{\bar{\gamma}}_b x + \bar{\bar{\gamma}}_b}{\bar{\bar{\gamma}}_b x}\right)\right). \tag{21}$$

Thus, for any chosen value of μ, the feasible constraints for having secure communication with positive confidential information rate must satisfy

$$\epsilon > \exp\left(-\frac{\min\{\mu, F(\mu, \delta)\}}{\bar{\gamma}_e}\right). \tag{22}$$

Note that when the reliability constraint is sufficiently loose, $F(\mu, \delta)$ becomes always greater than μ, and the above inequality changes to

$$\epsilon > \exp\left(-\frac{\mu}{\bar{\gamma}_e}\right). \tag{23}$$

From (22) or (23), we see that the on-off SNR threshold, μ, plays an important role in determining how strictly the security constraint can be set.

B. Adaptive-Rate Transmission Scheme

Now, we consider the scenario where the codeword transmission rate, R_b, and the confidential information rate, R_s, can be adaptively chosen according to the estimated instantaneous CSI of Bob's channel. In contrast to the fixed-rate transmission scheme, which requires only one-bit feedback, this scheme requires the feedback of the estimated instantaneous SNR. Since the confidential information rate, R_s, is adaptively chosen according to any given $\hat{\gamma}_b$, the system throughput for the adaptive-rate transmission scheme is given by

$$\eta = \int_{\mu}^{\infty} (1 - p_{co}) R_s f_{\hat{\gamma}_b}(\hat{\gamma}_b) \mathrm{d}\hat{\gamma}_b. \tag{24}$$

The lower limit of the integral in (24) is equal to μ, since the transmission takes place only when $\hat{\gamma}_b > \mu$ due to the on-off transmission scheme.

For any chosen values of R_b, R_s, and μ, the secrecy outage probability is given by (13). Since $\gamma_b \leq \hat{\gamma}_b$ and Bob can decode the message without error only when $C_b \geq R_b$, it is wise to choose the value of R_b satisfying $R_b \leq \log_2(1 + \hat{\gamma}_b)$. Then, for any given $\hat{\gamma}_b$, the connection outage probability can be computed as

$$\begin{aligned} p_{co}(R_b) &= \Pr(\log_2(1 + \gamma_b) < R_b | \hat{\gamma}_b) \\ &= \Pr\left(\log_2\left(1 + \frac{\hat{\gamma}_b}{\tilde{\gamma}_b + 1}\right) < R_b | \hat{\gamma}_b\right) \\ &= \Pr\left(\tilde{\gamma}_b > \frac{\hat{\gamma}_b}{2^{R_b} - 1} - 1 | \hat{\gamma}_b\right) \\ &= \exp\left(-\frac{1}{\bar{\bar{\gamma}}_b}\left(\frac{\hat{\gamma}_b}{2^{R_b} - 1} - 1\right)\right). \end{aligned} \tag{25}$$

Note that (25) is different from (15) in the fixed-rate transmission scheme, where (25) calculates the probability of connection outage for any given $\hat{\gamma}_b$ and (15) computes the probability of connection outage averaged over all possible values of $\hat{\gamma}_b$ ($\hat{\gamma}_b > \mu$).

Now we consider the design problem of finding the values of R_b, R_s and μ that maximize the throughput. Since R_b and R_s can be adaptively chosen according to any given $\hat{\gamma}_b$, we treat this design as a two-step optimization problem given by

Step 1: For any given $\hat{\gamma}_b$ ($\hat{\gamma}_b > \mu$), solve

$$\begin{aligned} \arg\max_{R_b, R_s} \quad & (1 - p_{co}(R_b)) R_s, \\ \text{s.t.} \quad & p_{so}(R_b, R_s) \leq \epsilon, p_{co}(R_b) \leq \delta, R_s > 0. \end{aligned}$$

Step 2: Choose the best μ to maximize the overall throughput averaged over $\hat{\gamma}_b$.

Since the values of R_b and R_s are adaptively chosen for any given $\hat{\gamma}_b$ in Step 1, we adopt (25) to calculate the connection outage probability such that the reliability constraint is satisfied for any given knowledge of Bob's estimated instantaneous CSI.

The following proposition summarizes the solution to the design problem for the adaptive-rate transmission scheme, where the optimal μ is given by a closed-form solution, the optimal R_s is expressed as a closed-form function of R_b and the optimal R_b is obtained by numerically solving an optimization problem.

Proposition 2: The optimal parameters for the adaptive-rate transmission scheme are given as follow:

$$\mu = \left(1 + \bar{\bar{\gamma}}_b \ln \delta^{-1}\right) \bar{\gamma}_e \ln \epsilon^{-1}. \tag{26}$$

$$R_s = R_b - k, \quad \textit{where} \quad k = \log_2(1 + \bar{\gamma}_e \ln \epsilon^{-1}). \tag{27}$$

R_b is obtained by solving the problem given by

$$\begin{aligned} \arg\max_{R_b} \quad & \left(1 - \exp\left(\frac{1}{\bar{\bar{\gamma}}_b}\left(1 - \frac{\hat{\gamma}_b}{2^{R_b} - 1}\right)\right)\right)(R_b - k), \\ \textit{s.t.} \quad & k < R_b \leq \log_2\left(1 + \frac{\hat{\gamma}_b}{1 + \bar{\bar{\gamma}}_b \ln \delta^{-1}}\right). \end{aligned}$$

Proof: For any chosen R_b, it is optimal to maximize R_s while satisfying $p_{so}(R_b, R_s) \leq \epsilon$. Hence, the optimal R_s is given as (27). To satisfy $R_s > 0$ and $p_{co}(R_b) \leq \delta$, we obtain the lower and upper bounds of R_b given by $R_b > k$ and $R_b \leq \log_2\left(1 + \frac{\hat{\gamma}_b}{1 + \bar{\bar{\gamma}}_b \ln \delta^{-1}}\right)$. Thus, the optimal R_b can be obtained by solving the optimization problem given in Proposition 2. To obtain the optimal μ, we start from looking for the range of $\hat{\gamma}_b$ in which it is possible to have secure communication with positive confidential information rate while satisfying both constraints. Let the lower bound of R_b be less than the upper bound of R_b, we can find the feasible range of $\hat{\gamma}_b$ as

$$\begin{aligned} & \log_2\left(1 + \bar{\gamma}_e \ln \epsilon^{-1}\right) < \log_2\left(1 + \frac{\hat{\gamma}_b}{1 + \bar{\bar{\gamma}}_b \ln \delta^{-1}}\right) \\ & \Leftrightarrow \hat{\gamma}_b > \left(1 + \bar{\bar{\gamma}}_b \ln \delta^{-1}\right) \bar{\gamma}_e \ln \epsilon^{-1}. \end{aligned} \tag{28}$$

Thus, the optimal μ is equal to the lower bound of the feasible $\hat{\gamma}_b$, given by (26). ■

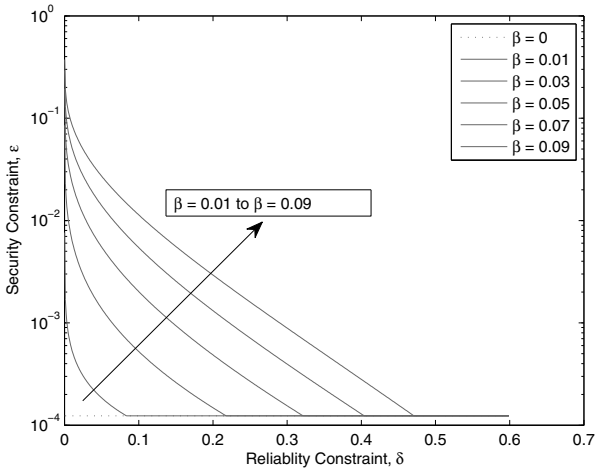

Fig. 1. Fixed-rate transmission scheme: the feasible security constraint versus reliability constraint. Results are shown for networks with different variances of channel estimation error, i.e., $\beta = 0, 0.01, 0.03, 0.05, 0.07, 0.09$. The other system parameters are $\mu = 9$, $P_b = 10$ dB, $P_e = 0$ dB.

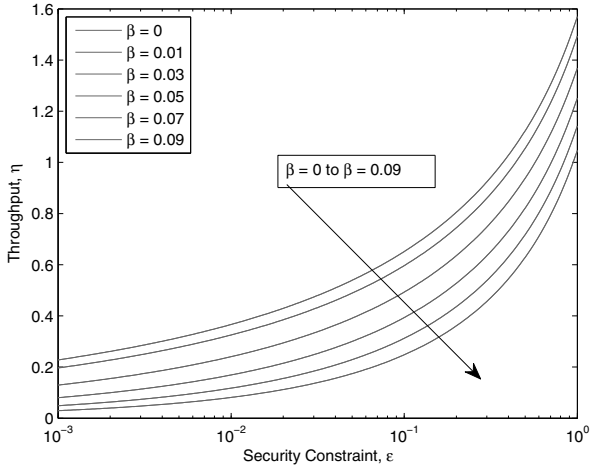

Fig. 2. Fixed-rate transmission scheme: the achievable throughput of secure transmission versus the security constraint. Results are shown for networks with different variances of the channel estimation error, $\beta = 0, 0.01, 0.03, 0.05, 0.07, 0.09$. The other system parameters are $\delta = 0.1$, $P_b = 10$ dB, $P_e = 0$ dB.

From Proposition 2, one can further obtain that the optimal R_b should be equal to either the upper bound of R_b, i.e., $R_b = \log_2\left(1 + \frac{\hat{\gamma}_b}{1+\bar{\tilde{\gamma}}_b \ln \delta^{-1}}\right)$, or some value that satisfies the equation

$$\frac{\mathrm{d}I(R_b)}{\mathrm{d}R_b} = 1 - \exp\left(\frac{1}{\bar{\tilde{\gamma}}_b} - \frac{\hat{\gamma}_b}{\bar{\tilde{\gamma}}_b\left(2^{R_b}-1\right)}\right) \cdot \left(1 + \frac{2^{R_b}\hat{\gamma}_b\left(R_b - k\right)\ln 2}{\bar{\tilde{\gamma}}_b\left(2^{R_b}-1\right)^2}\right) = 0 \tag{29}$$

where $I(R_b) = \left(1 - \exp\left(\frac{1}{\bar{\tilde{\gamma}}_b}\left(1 - \frac{\hat{\gamma}_b}{2^{R_b}-1}\right)\right)\right)(R_b - k)$. Note that when $\bar{\tilde{\gamma}}_b = 0$, $\hat{\gamma}_b = \gamma_b$, Proposition 2 implies that $R_b = \log_2(1+\gamma_b)$, which is consistent with the optimal solution of R_b in the absence of the estimation error (i.e., the optimal codeword rate matches the capacity of Bob's channel.).

IV. Numerical Results and Discussion

In this section, we present the numerical results to illustrate how the channel estimation error affects the achievable secure transmission throughput and constraints. We show the results for the networks with variances of the channel estimation error in the range from $\beta = 0$, i.e, the channel is perfectly estimated, to around $\beta = 0.1$. The average SNR of the received signal (without the consideration of channel uncertainty) at Bob and Eve are set as $P_b = 10$ dB and $P_e = 0$ dB, respectively[2].

Fig. 1 illustrates the feasible security and reliability constraints under which it is possible to have secure communication with positive confidential information rate in the fixed-rate transmission scheme. The networks with different variances of channel estimation error are represented by different curves.

[2]When P_e is comparable or larger than P_b, the achievable throughput is very small or reaches zero. In order to achieve better performance in such a scenario, one can consider multi-antenna transmission or using external helpers to regain the relative advantage of the legitimate receiver's channel over the eavesdropper's channel.

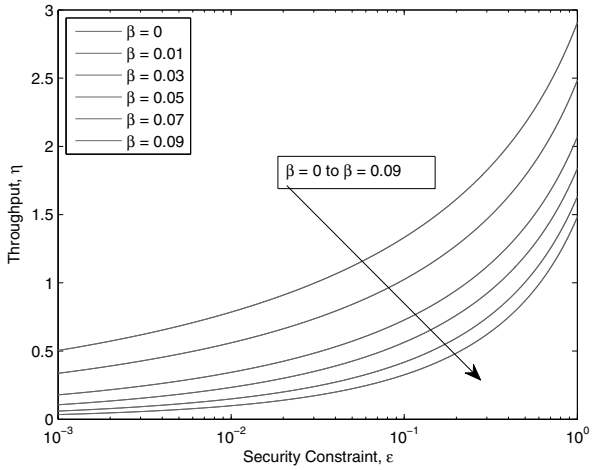

Fig. 3. Adaptive-rate transmission scheme: the achievable throughput of secure transmission versus the security constraint. Results are shown for networks with different variances of the channel estimation error, $\beta = 0, 0.01, 0.03, 0.05, 0.07, 0.09$. The other system parameters are $\delta = 0.1$, $P_b = 10$ dB, $P_e = 0$ dB.

Besides, the on-off SNR threshold is fixed to $\mu = 9$. For each network, the feasible constraints lie in the region above the corresponding curve. As depicted in the figure, when the reliability constraint goes loose (as δ increases), the network can achieve stricter security constraint (as a smaller ϵ is achievable). The lower bound on the feasible value of ϵ is related to the on-off SNR threshold as given in Eq. (23). Comparing the curves, we find that, subject to the same reliability constraint, the networks with smaller variances of channel estimation error can achieve stricter security constraints.

Figs. 2 and 3 present the achievable throughput over a range of security constraints for networks with different channel estimation error variances. Fig. 2 illustrates the results for the fixed-rate transmission scheme and Fig. 3 demonstrates the

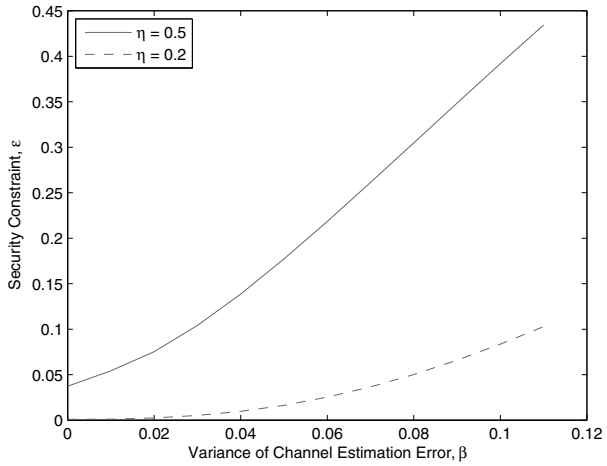

Fig. 4. Fixed-rate transmission scheme: the achievable security constraint versus the variance of the channel estimation error. Results are shown for networks with different target throughput values, i.e., $\eta = 0.5, 0.2$. The other parameters are $\delta = 0.1$, $P_b = 10$ dB, $P_e = 0$ dB.

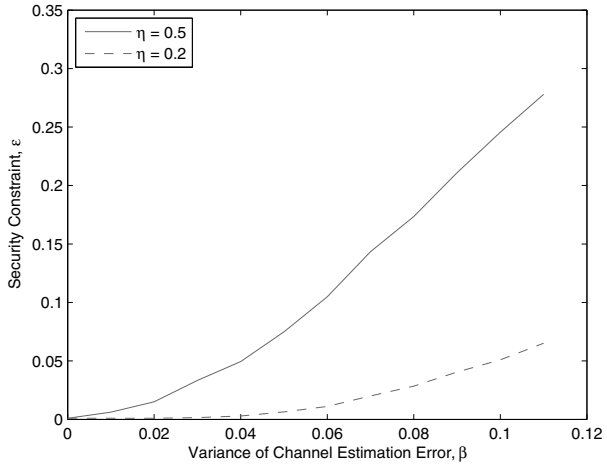

Fig. 5. Adaptive-rate transmission scheme: the achievable security constraint versus the variance of the channel estimation error. Results are shown for networks with different target throughput values, i.e., $\eta = 0.5, 0.2$. The other parameters are $\delta = 0.1$, $P_b = 10$ dB, $P_e = 0$ dB.

results for the adaptive-rate transmission scheme. For both schemes, the reliability constraint is fixed to $\delta = 0.1$. As shown in the figures, the achievable throughput increases with the decrease of the variance of the channel estimation error. Comparing these two figures, we find that, adaptively changing the rates of the transmitted codewords and the confidential data based on the knowledge of the estimated instantaneous CSI considerably improves the achievable throughput. While, the fixed-rate transmission scheme, which requires only one-bit feedback, minimizes the required feedback information.

Figs. 4 and 5 show the impact of channel estimation error on the achievable security level with a target throughput. Fig. 4 depicts the results for the fixed-rate transmission scheme and Fig. 5 presents the results for the adaptive-rate transmission scheme. As shown in the figures, when the variance of the channel estimation error increases, we have to loose the security constraint in order to achieve the target throughput. In addition, we see that the slopes of curves keep small, as the variance of the channel estimation error increases from 0 to some small value, e.g., 0.03. In other words, the security cost for maintaining the target throughput with a poorer channel estimation is low when the amount of channel estimation error is small. On the other hand, once the variance of the channel estimation error becomes relatively large, the slopes of curves go large. This implies that the security cost is high when the channel estimation error becomes considerable. Take the fixed-rate transmission scheme with target throughout equal to 0.5 as an example: When the variance of the channel estimation error increases from 0 to 0.02, the value of ϵ increases by 0.0384. However, when the variance of the channel estimation error increases from 0.04 to 0.06, the value of ϵ increases by 0.0798, which is larger than twice as much as 0.0384.

V. Conclusion

We studied the problem of secure transmission design under the assumption that the legitimate receiver's instantaneous CSI is imperfectly known due to channel estimation errors. Based on the different amounts of feedback information at the transmitter, two on-off secure transmission schemes, the fixed-rate scheme and the adaptive-rate scheme, were proposed. For both transmission schemes, the optimal on-off SNR threshold as well as the optimal rates of transmitted codewords and confidential information were provided as the solution to a throughput maximization problem. Our numerical results showed that the presence of channel estimation error reduces the achievable throughput or the achievable security level. For achieving a fixed target throughput, the security cost of having a small amount of channel estimation error is relatively low. While, the security cost becomes considerable when the channel estimation error starts to become large.

References

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

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

[3] J. 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 Workshop on CAMAD*, Kyoto, Japan, June 2011, pp. 122–126.

[4] X. Zhou and M. Mckay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 3831 – 3842, Oct. 2010.

[5] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, pp. 351 – 361, Jan. 2011.

[6] A. Vakili, M. Sharif, and B. Hassibi, "The effect of channel estimation error on the throughput of broadcast channels," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Process.*, vol. 4, Toulouse, France, May 2006.

[7] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[8] X. Tang, R. Liu, Sapsojević, and H. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1590, Apr. 2009.

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