Secure Beamforming Transmission with Limited Training and Feedback

Jianwei Hu*, Yueming Cai*, Nan Yang†, Xiangyun Zhou† and Weiwei Yang*
College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China*
Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia†

***Abstract*—We consider the secure beamforming transmission over a quasi-static block fading channel from a multi-antenna transmitter to a desired single-antenna receiver, in the presence of a passive single-antenna eavesdropper. We focus on a practical scenario where the transmitter can only acquire the statistical channel knowledge of the eavesdropper and the partial channel knowledge of the legitimate receiver through a finite amount of signaling overhead. To keep control of the outage events caused by the limited channel knowledge, We firstly propose a strategy to determine the wiretap code parameters under the outage constraints, based on which we establish a necessary transmission condition to guarantee a positive secrecy rate. Aided by this transmission condition, we propose an on-off-based transmission scheme and characterize the secrecy throughput performance of the system. Our designed transmission scheme is beneficial for the deployment of physical layer security in practical frequency division duplex (FDD) systems with limited training and feedback.**

***Index Terms*—Secure beamforming, on-off transmission, limited training and feedback overhead.**

I. Introduction

Over the past few years, there has been an increased interest in physical layer security to protect the wireless communications against eavesdropping. The seminal work in this area can be traced back to Wyner, who concluded in [1] that secure communication can be achieved at the physical layer. This conclusion has fueled much research work to investigate *physical layer security*. Many of these early studies have in common that the transmitter can obtain perfect channel state information (CSI). Such idealized conditions bring us attractive advantages. However, since the training and feedback overhead is practically limited, the transmitter can never obtain perfect channel knowledge of the receiver and/or the eavesdropper [2].

Recently, there has been several studies that have designed practical secure transmission schemes under imperfect CSI [3–6]. Specifically, considering the channel estimation errors, the on-off mechanism was adopted to design an practical secure transmission scheme [3]. Focusing on the quantized channel feedback, the artificial-noise-aided beamforming scheme was optimized to guarantee security for the fast fading channels [4] and the slow fading channels [5]. For block fading channels, the non-trivial tradeoff between the signaling overhead and the effective data transmission in wiretap channels was characterized in [6], which defined the effective ergodic secrecy rate (ESR) as the performance metric and investigated the optimization problem for maximization of effective ESR.

In this paper, we consider the multi-input single-output single-eavesdropper (MISOSE) scenario in block fading channels and concentrate on a practical CSI assumption that the transmitter can only obtain the statistical channel knowledge to the eavesdropper and partial channel knowledge to the legitimate receiver through finite signaling overhead. Due to this imperfect channel knowledge, there inevitably occurs two kinds of practical issues, i.e., connection outage event and secrecy outage event. The former is due to the lack of perfect channel knowledge of the legitimate receiver, while the latter is due to the lack of perfect channel knowledge of the eavesdropper. To guarantee the target levels of reliability and security in the considered wiretap channel, we design an on-off-based secure beamforming transmission scheme under dual outage constraints. In particular, we first establish a necessary transmission condition on the channel knowledge known at the transmitter to ensure that a positive secrecy rate is available under dual outage constraints. That is, the transmission should be allowed only when the quality of the main channel is larger than the designated threshold. Built upon this condition, we then design an on-off secure transmission scheme and characterize the secrecy throughput by averaging the secrecy rate over all channel realizations.

The rest of this paper is organized as follows. In Section II, we provide an overview of the MISOSE scenario with training and feedback overhead. In Section III, we characterize the connection and secrecy outage performance. In Section IV, we design the on-off transmission scheme under dual outage constraints. In Section V and VI, we present some numerical simulations and summarize our main findings.

II. System Model

We consider a MISOSE scenario where the M-antenna transmitter (Alice) communicates with a desired single-antenna receiver (Bob) in the presence of a passive single-antenna eavesdropper (Eve). The Alice-Bob link is referred to as the main channel, and the Alice-Eve link is referred to as the eavesdropper's channel. A quasi-static Rayleigh block fading model is assumed such that the channel coefficients are independent identically distributed (i.i.d) complex Gaussian random variables with zero mean and unit variance across the coherence blocks, but hold constant for a certain transmission block before changing independently.

In this work, we consider a practical scenario, where Eve is just an ordinary user of the network whose detection performance has no prior to Bob, such that Eve performs the same as Bob to estimate her channel by computing a minimum mean square error (MMSE) estimation based on the training symbols. After the channel estimation process, Bob uses the noisy channel estimation to choose the *nearest* transmit beamforming vector from a codebook known a prior at Alice and Bob, and then feeds back the index of associated beamformer vector to Alice. Since Eve behaves as a passive eavesdropper, the instantaneous knowledge of the eavesdropper's channel cannot be acquired by Alice.

A. System Input-Output Relationship

We assume that Alice transmits a modulated symbol s chosen from a constellation S with unit variance. Before transmission on antenna i, the symbol is weighted by a complex number v_i. The weights for all antennas can be collected into an $M \times 1$ unitary beamforming vector $\mathbf{v} = [v_1, v_2, \cdots, v_M]^T$. Let h_i denote the channel coefficient between the single received antenna at Bob and the i-th transmit antenna at Alice, such that $h_i \sim \mathcal{CN}(0,1)$ and the main channel vector is $\mathbf{h} = [h_1, h_2, \cdots, h_M]$. Thus the received symbol at Bob is written as

$$y = \mathbf{h}\mathbf{v}s + n_b, \tag{1}$$

where n_b is the additive white Gaussian noise (AWGN) at Bob with variance σ_b^2.

Furthermore, we denote g_i as the channel coefficient between the single received antenna at Eve and the i-th transmit antenna at Alice, such that $g_i \sim \mathcal{CN}(0,1)$ and the eavesdropper's channel vector is $\mathbf{g} = [g_1, g_2, \cdots, g_M]$. As such, the received symbol at Eve is written as

$$z = \mathbf{g}\mathbf{v}s + n_e, \tag{2}$$

where n_e is the AWGN at Eve with variance σ_e^2.

B. Training and Feedback Process

In this subsection, we describe the detailed process of how Alice acquires the actual CSI by exploiting the finite training and feedback overhead.

1) Channel Estimation at Bob and Eve: We assume that Bob computes the linear MMSE estimation of $\mathbf{h}$ given T training symbols, such that we have $\mathbf{h} = \hat{\mathbf{h}} + \mathbf{m}$, where the estimated channel $\hat{\mathbf{h}}$ and the estimated error $\mathbf{m}$ contain i.i.d complex Gaussian elements, satisfying $\hat{\mathbf{h}} \sim \mathcal{CN}\left(0, (1-\sigma_m^2)\mathbf{I}_M\right)$ and $\mathbf{m} \sim \mathcal{CN}\left(0, \sigma_m^2 \mathbf{I}_M\right)$, respectively. According to [7], σ_m^2 is formulated as

$$\sigma_m^2 = \frac{1}{1+\rho_b \bar{T}}. \tag{3}$$

where $\rho_b = 1/\sigma_b^2$ denotes the average signal-to-noise (SNR) of the received signal at Bob without estimation error, and $\bar{T} = T/M$ is the normalized number of training symbols.

Also, Eve computes the linear MMSE estimation of $\mathbf{g}$ as $\mathbf{g} = \hat{\mathbf{g}} + \mathbf{w}$, where the estimated channel $\hat{\mathbf{g}}$ and the estimated error $\mathbf{w}$ contain i.i.d complex Gaussian elements, satisfying $\hat{\mathbf{g}} \sim \mathcal{CN}\left(0, (1-\sigma_w^2)\mathbf{I}_M\right)$ and $\mathbf{w} \sim \mathcal{CN}\left(0, \sigma_w^2 \mathbf{I}_M\right)$, respectively. Similar to (3), σ_w^2 is given by

$$\sigma_w^2 = \frac{1}{1+\rho_e \bar{T}}, \tag{4}$$

where $\rho_e = 1/\sigma_e^2$ denotes the average SNR of the received signal at Eve without estimation error.

2) Quantization at Bob: After channel estimation process, Bob needs to convey back the index of the particular beamforming vector to Alice via B bits over a feedback channel. Specifically, Bob selects the SNR-maximizing beamforming vector $\mathbf{v}$ from a codebook $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{2^B}\}$, yielding

$$\mathbf{v} = \arg\max_{\mathbf{f}_i \in \mathcal{V}} |\hat{\mathbf{h}}\mathbf{f}_i|^2, \tag{5}$$

after which the index of the selected beamforming vector is fed back to Alice.

After the CDI feedback process, Bob also needs to convey back the CQI to Alice. Different from the CDI quantization, which needs many feedback bits especially when M is very large, the CQI is just a positive real number and can be quantized efficiently using a small number of bits [5, 8, 9]. As such, to concentrate on the impact of CDI quantization, in this work we assume that Alice can perfectly obtain the CQI without consuming the block resources.

C. Wiretap Codes Design

We now construct a parameter pair (R_b, R_e) for the wiretap code [1], where R_b denotes the codeword transmission rate and R_e denotes the rate redundancy which provides secrecy against eavesdropping. To guarantee the reliability and security levels, in this work we choose the largest possible codeword rate R_b while keeping the required reliability level at Bob, and we also choose the smallest possible rate redundancy R_e while providing the required security level against eavesdropping, both from a probabilistic sense [5]. By doing so, we maximize the achievable secrecy rate ($R_s = R_b - R_e$), while the risks of decoding error and being eavesdropped are both under control.

III. Outage Performance Analysis

In this section, we characterize the dual outage probabilities, i.e., the connection outage probability and the secrecy outage probability. Specifically, by designing a *back off* strategy to determine the codeword rate, we present a brief expression to calculate the connection probability. Furthermore, given a predetermined rate redundancy, we derive the closed-form expression for the secrecy outage probability.

A. Connection Outage Probability

We first characterize the instantaneous SNR of the main channel. Based on the channel estimation and limited feedback model in Section II-B, we rewrite (1) as

$$y = (\hat{\mathbf{h}} + \mathbf{m})\mathbf{v}s + n_b = \hat{\mathbf{h}}\mathbf{v}s + \mathbf{m}\mathbf{v}s + n_b. \tag{6}$$

Note that the estimate $\hat{\mathbf{h}}$ and the selected beamforming vector $\mathbf{v}$ are known at Bob. Therefore, Bob can exploit $\hat{\mathbf{h}}\mathbf{v}$ for data detection, and thus the actual instantaneous SNR of the main channel is given by

$$\gamma_b = \frac{\rho_b |\hat{\mathbf{h}}\mathbf{v}|^2}{\rho_b |\mathbf{m}\mathbf{v}|^2 + 1}. \tag{7}$$

We define $v = |\hat{\mathbf{h}}\mathbf{v}|^2/\|\hat{\mathbf{h}}\|^2$, $\hat{\gamma}_b = \rho_b \|\hat{\mathbf{h}}\|^2$ and $\tilde{\gamma}_b = \rho_b |\mathbf{m}\mathbf{v}|^2$, and rewrite (7) as

$$\gamma_b = \frac{v\hat{\gamma}_b}{\tilde{\gamma}_b + 1}. \tag{8}$$

In this work we adopt the codebook design criterion presented in [9–11], such that the cumulative density distribution (CDF) of v in (8) can be approximated as

$$F_v(x) = \begin{cases} 0, & 0 \le x \le 1-\varepsilon \\ 1 - N(1-x)^{M-1}, & 1-\varepsilon \le x \le 1 \end{cases} \tag{9}$$

where $\varepsilon = 2^{-\frac{B}{M-1}}$ and $N = 2^B$. We also present the statistics of $\hat{\gamma}_b$ and $\tilde{\gamma}_b$ to facilitate our performance analysis. We define $\alpha_b = \rho_b \left(1 - \sigma_m^2\right)$ and $\beta_b = \rho_b \sigma_m^2$, such that the CDF of $\hat{\gamma}_b$ and $\tilde{\gamma}_b$ can be written as

$$F_{\hat{\gamma}_b}(x) = 1 - \exp\left(-\frac{x}{\alpha_b}\right) \sum_{m=0}^{M-1} \frac{(x/\alpha_b)^m}{\Gamma(m+1)} \tag{10}$$

and

$$F_{\tilde{\gamma}_b}(x) = 1 - \exp\left(-\frac{x}{\beta_b}\right), \tag{11}$$

respectively. Aided by (11), we further find that the distribution of the actual SNR (i.e., γ_b) conditioned on its quantized estimation (i.e., $v\hat{\gamma}_b$) can be written as

$$F_{\gamma_b|v\hat{\gamma}_b}(y\,|x) = \exp\left(-\frac{1}{\beta_b}\left(\frac{x}{y} - 1\right)\right) u\left(\frac{x}{y} - 1\right), \tag{12}$$

where $u(\cdot)$ denotes the unit step function.

Here, we propose such a *back off* strategy: Given a certain CQI, Alice backs off from $v\hat{\gamma}_b$ to $\gamma_{backoff} = v\hat{\gamma}_b/\mu$ and sends at a rate of $\log(1 + \gamma_{backoff})$, where μ is the back off factor and $\mu > 1$. Clearly, if γ_b falls blow $\gamma_{backoff}$, the connection outage event occurs. Thus for a given CQI, the connection outage probability can be formulated as

$$p_{co} = \Pr\left\{\gamma_b < \gamma_{backoff}\,|v\hat{\gamma}_b\right\}. \tag{13}$$

With the aid of (12), we derive p_{co} as

$$p_{co} = F_{\gamma_b|v\hat{\gamma}_b}\left(\frac{v\hat{\gamma}_b}{\mu}\,|v\hat{\gamma}_b\right) = \exp\left(-\frac{\mu - 1}{\beta_b}\right). \tag{14}$$

Based on (14), we find that the expression for p_{co} is independent of the CQI. That is, our proposed *back off* design provides an easy expression to determine the connection outage probability.

B. Secrecy Outage Probability

Considering the MMSE estimator at Eve, the received signal at Eve can be written as

$$z = (\hat{\mathbf{g}} + \mathbf{w})\mathbf{v}s + n_e = \hat{\mathbf{g}}\mathbf{v}s + \mathbf{w}\mathbf{v}s + n_e. \tag{15}$$

Based on (15), the instantaneous SNR of the eavesdropper's channel is given by

$$\gamma_e = \frac{\rho_e |\hat{\mathbf{g}}\mathbf{v}|^2}{\rho_e |\mathbf{w}\mathbf{v}|^2 + 1}. \tag{16}$$

We define $\hat{\gamma}_e = \rho_e |\hat{\mathbf{g}}\mathbf{v}|^2$ and $\tilde{\gamma}_e = \rho_e |\mathbf{w}\mathbf{v}|^2$, and thus (16) can be rewritten as

$$\gamma_e = \frac{\hat{\gamma}_e}{\tilde{\gamma}_e + 1}. \tag{17}$$

Note that $\mathbf{v}$ is completely determined by Bob's estimated channel vector $\hat{\mathbf{h}}$. Thus $\mathbf{v}$ is independent of the Eve's estimated channel vector $\hat{\mathbf{g}}$ and error vector $\mathbf{w}$. Furthermore, since $\mathbf{v}$ is an unitary vector, both $\hat{\mathbf{g}}\mathbf{v}$ and $\hat{\mathbf{w}}\mathbf{v}$ are i.i.d. complex Gaussian entries with variance $1 - \sigma_w^2$ and σ_w^2, respectively. Therefore, the CDF of γ_e in (17) is derived as

$$\begin{aligned} F_{\gamma_e}(x) &= \int_0^\infty F_{\hat{\gamma}_e}\left((1+y)\,x\right) f_{\tilde{\gamma}_e}(y)\,dy \\ &= 1 - \frac{\alpha_e}{\alpha_e + \beta_e x} \exp\left(-\frac{x}{\alpha_e}\right), \end{aligned} \tag{18}$$

where $\alpha_e = \rho_e \left(1 - \sigma_w^2\right)$ and $\beta_e = \rho_e \sigma_w^2$.

For a given rate redundancy R_e, the secrecy outage probability can be formulated as

$$\begin{aligned} p_{so} &= \Pr\left\{R_e < C_e\right\} = \Pr\left\{2^{R_e} - 1 < \gamma_e\right\} \\ &= \frac{\alpha_e}{\alpha_e + \beta_e\left(2^{R_e} - 1\right)} \exp\left(-\frac{2^{R_e} - 1}{\alpha_e}\right). \end{aligned} \tag{19}$$

In this work we assume that Eve's instantaneous channel knowledge is not available at Alice, but her statistical channel knowledge (i.e., ρ_e) can be acquired by Alice. In the literature, this assumption of available knowledge about ρ_e has been stated in other secrecy studies, e.g. [12–15].

IV. Secure Transmission Design

In this section, we design the secure transmission scheme under a connection constraint (i.e., ϵ) and a secrecy outage constraint (i.e., δ), respectively. We first present the condition on CQI, which guarantees a positive secrecy rate under dual outage constraints. We then investigate the secrecy throughput performance by averaging the secrecy rate over all CQI realizations.

A. Condition for Secure Transmission

Under dual connection and secrecy outage constraints, a positive secrecy rate is not always available. Therefore, we first establish the necessary and sufficient condition on the system parameters to guarantee that a positive R_s is achievable.

Proposition 1: To achieve a positive confidential rate, the CQI of the main channel must satisfy

$$\mathrm{CQI} > \gamma_{th} = \left(1 + \beta_b \ln \epsilon^{-1}\right) \alpha_e \ln \delta^{-1} \tag{20}$$

Proof: For a given CQI (i.e., $v\hat{\gamma}_b$), the maximum allowable codeword rate implies the minimum back off factor. That is, we have $R_{b,max} = \log(1 + v\hat{\gamma}_b/\mu_{\min})$. By observing (14), we find that under the connection outage constraint $p_{co} \leq \epsilon$, the minimum back off factor is

$$\mu_{\min} = 1 + \beta_b \ln \epsilon^{-1}. \tag{21}$$

With the aid of (19), we show that under the secrecy outage constraint $p_{so} \leq \delta$, the minimum required rate redundancy is $R_{e,\min} = \log(1 + \Theta)$, where Θ is the non-trivial solution to the following equation:

$$\delta = \frac{\alpha_e}{\alpha_e + \beta_e \Theta} \exp\left(-\frac{\Theta}{\alpha_e}\right). \tag{22}$$

Although it is not tractable to determine an analytical solution for Θ, however, we find that the upper bound of Θ can be formulated as $\Theta_{ub} = \alpha_e \ln \delta^{-1}$. Towards a robust design, in this work we exploit the upper bound of $R_{e,\min}$ as the minimum required rate redundancy, given by

$$R_{e,\min}^{ub} = \log\left(1 + \alpha_e \ln \delta^{-1}\right). \tag{23}$$

To ensure that a positive secrecy rate is available, $R_{b,max} > R_{e,\min}^{ub}$ must be always satisfied. Based on (21) and (23), we find that $R_{b,max} > R_{e,\min}^{ub}$ means that $v\hat{\gamma}_b/\mu_{\min} > \alpha_e \ln \delta^{-1}$ is required. As such, we establish ***Proposition 1***. ■

From a design perspective, ***Proposition 1*** implies that the "on-off" transmission scheme with the threshold γ_{th} in (20) is appropriate for our system. As such, in what follows we adopt the on-off scheme to perform our transmission design.

B. On-Off Transmission Scheme

In this work, the on-off transmission strategy is operated as following: when the CQI known at Alice is larger than γ_{th}, Alice starts to perform secure transmission with rate parameters $R_{b,max}$ and $R_{e,\min}^{ub}$ in (23). Thus the achievable secrecy rate for a given CQI is

$$R_s(v\hat{\gamma}_b) = R_b - R_e = \log\left(\frac{1 + v\hat{\gamma}_b/\mu_{\min}}{1 + \alpha_e \ln \delta^{-1}}\right). \tag{24}$$

By applying such a strategy to determine the rate parameters, we observe that $p_{co} = \epsilon$ is always true by substituting $\mu_{\min}$ into (14). However, by substituting $R_{e,\min}^{ub}$ into (19), the secrecy outage probability is formulated as

$$p_{so} = \frac{\delta}{1 - \beta_e \ln \delta}, \tag{25}$$

which is always less than δ. Based on (25), we find that the secrecy outage probability successively approximates δ as we go along increasing the pilot length T.

Next, we incorporate the connection outage and secrecy outage probabilities 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. The secrecy throughput, η, is defined as

$$\eta = p_{r\&s} \int_{\gamma_{th}}^{\infty} R_s(x) f_{v\hat{\gamma}_b}(x)\, dx, \tag{26}$$

where $p_{r\&s} = (1 - p_{co})(1 - p_{so})$ denotes the reliable and secure transmission probability, and $f_{v\hat{\gamma}_b}(x)$ is the probability density function (PDF) of $v\hat{\gamma}_b$, given by

$$\begin{aligned} f_{v\hat{\gamma}_b}(x) =& \frac{N}{\alpha_b} \exp\left(-\frac{x}{\alpha_b}\right) - \frac{N}{\alpha_b} \exp\left(-\frac{x}{(1-\varepsilon)\alpha_b}\right) \\ &\times \sum_{m=0}^{M-2} \frac{1}{\Gamma(m+1)} \left(\frac{\varepsilon x}{(1-\varepsilon)\alpha_b}\right)^m. \end{aligned} \tag{27}$$

The proof is given in Appendix A.

Substituting (27) into (26), we derive the secrecy throughput as

$$\eta = \frac{(1-\epsilon)}{\ln 2}\left(1 - \frac{\delta}{1 - \beta_e \ln \delta}\right)(\ell_1 + \ell_2), \tag{28}$$

where ℓ_1 is

$$\ell_1 = -N \exp\left(\frac{\mu_{min}}{\alpha_b}\right) \mathrm{Ei}\left(-\frac{\mu_{min}(1 - \alpha_e \ln \delta)}{\alpha_b}\right), \tag{29}$$

ℓ_2 is

$$\begin{aligned} \ell_2 =& \exp\left(\frac{\mu_{\min}}{(1-\varepsilon)\alpha_b}\right) \sum_{m=0}^{M-1} \sum_{n=0}^{m} \left(-\frac{\mu_{\min}}{(1-\varepsilon)\alpha_b}\right)^{m-n} \\ &\times \frac{(1 - N\varepsilon^m)\Psi_n}{\Gamma(n+1)\Gamma(m-n+1)}, \end{aligned} \tag{30}$$

and Ψ is

$$\Psi_n = \begin{cases} -\mathrm{Ei}\left(-\frac{\mu_{\min}\left(1+\alpha_e \ln \delta^{-1}\right)}{(1-\varepsilon)\alpha_b}\right), & n = 0 \\ \Gamma\left(n, \frac{\mu_{\min}\left(1+\alpha_e \ln \delta^{-1}\right)}{(1-\varepsilon)\alpha_b}\right), & n \geq 1 \end{cases} \tag{31}$$

respectively. We clarify that $\mathrm{Ei}(\cdot)$ is the Exponential integral function defined in [16, Eq. (8.211)], and $\Gamma(\cdot,\cdot)$ is the incomplete Gamma function defined in [16, Eq. (8.352)].

C. Secrecy Throughput Loss Caused by Limited Feedback

We clarify that limited feedback comes with some performance loss of the secrecy throughput compared with the adaptation techniques with perfect channel information via unlimited feedback. We now characterize this performance loss. First, we formulate the secrecy throughput with perfect CDI feedback (i.e., $v = 1$) as

$$\eta_{v=1} = p_{r\&s} \int_{\gamma_{\text{th}}}^{\infty} R_s(x) f_{\hat{\gamma}_b}(x)\, dx, \tag{32}$$

where $f_{\hat{\gamma}_b}$ can be derived by taking the first order derivative of $F_{\hat{\gamma}_b}$ given by (10). Using the similar method of mathematical derivation for η in (28), $\eta_{v=1}$ is obtained as

$$\begin{aligned} \eta_{v=1} =& \frac{(1-\epsilon)}{\ln 2}\left(1 - \frac{\delta}{1 - \beta_e \ln \delta}\right) \exp\left(\frac{\mu}{\alpha_b}\right) \sum_{m=0}^{M-1} \sum_{l=0}^{m} \Xi_l \\ &\times \frac{1}{\Gamma(l+1)\Gamma(m-l+1)} \left(-\frac{\mu_{min}}{\alpha_b}\right)^{m-l}, \end{aligned} \tag{33}$$

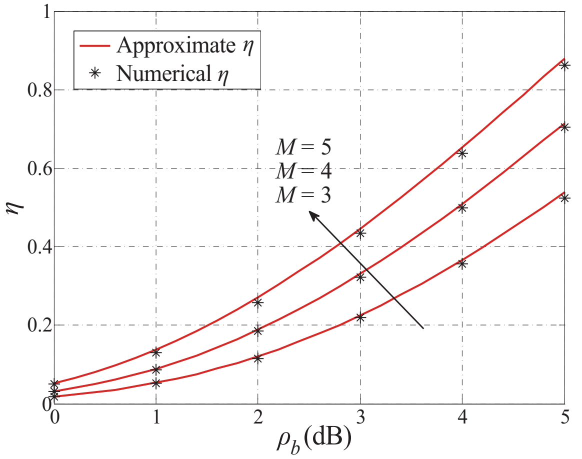

Fig. 1. Secrecy throughput versus ρ_b for $\rho_e = 0$ dB, $\bar{T} = 2$, $B = M$, $\epsilon = 0.1$ and $\delta = 0.1$.

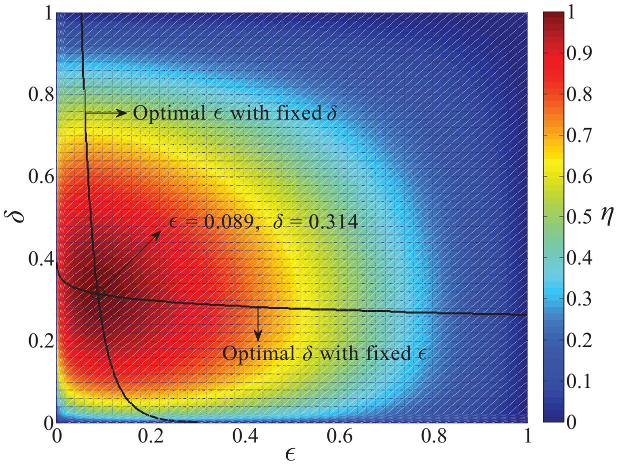

Fig. 2. Secrecy throughput versus ϵ and δ for $\rho_b = 3$ dB, $\rho_e = 0$ dB, $M = 4$, $T = 20$ and $B = 5$.

where Ξ is given by

$$\Xi_l = \begin{cases} -\mathrm{Ei}\left(-\frac{\mu_{\min}\left(1+\alpha_e \ln \delta^{-1}\right)}{\alpha_b}\right), & l = 0 \\ \Gamma\left(l, \frac{\mu_{\min}\left(1+\alpha_e \ln \delta^{-1}\right)}{\alpha_b}\right), & l \geq 1 \end{cases} \tag{34}$$

Based on (28) and (33), we find that $\eta_{\Delta} = \eta_{v=1} - \eta$ is the secrecy throughput loss caused by the limited feedback.

V. Numerical Results

In this section, we give some numerical results to examine the accuracy of our above analysis and show the impact of the outage constraints on system performance.

It is worth mentioning that for the derivation of the secrecy throughput in (28), the approximated CDF of v was used. That is, (28) is also an approximate expression. To characterize the accuracy level of this approximation, Fig. 1 plots the approximate secrecy throughput versus ρ_b for different values of transmit antenna number M, along which the accurate secrecy throughput are provided with Monte Carlo simulation results. The quantization codebook is generated based on the design criterion in [9–11]. As can be seen, the differences between the exact results and our analytical approximations are almost negligible. That is, the considered quantization approximation has only a negligible effect on the secrecy throughput. As such, the closed-form expression (28) derived based on the quantization approximation can accurately predict the secrecy throughput with training and limited feedback.

Note that in Fig. 1 the dual outage constraints are fixed to 0.1. One may also want to know the impact of the specific choice of ϵ and δ on the secrecy throughput performance. This is investigated in Fig. 2, which plots the secrecy throughput versus the connection and secrecy outage constraints. Since Monte Carlo simulation requires an exhaustive search over the codebook, and the number of entries in the codebook grows exponentially with the number of feedback bits, simulation results are not shown in this figure. We first observe that the secrecy throughput reaches its maximum value at $(\epsilon = 0.089, \delta = 0.314)$ and decays gradually toward the edge. We further observe that for a fixed ϵ (or δ), the optimal δ (or ϵ) maximizing the secrecy throughput decreases continuously along with the ϵ (or δ) increasing. In particular, the two black lines in Fig. 2 show that the optimal δ decreases from 0.39 to 0.26 when ϵ increases from 0 to 1; while the optimal ϵ decreases from 0.30 to 0.05 when δ increases from 0 to 1.

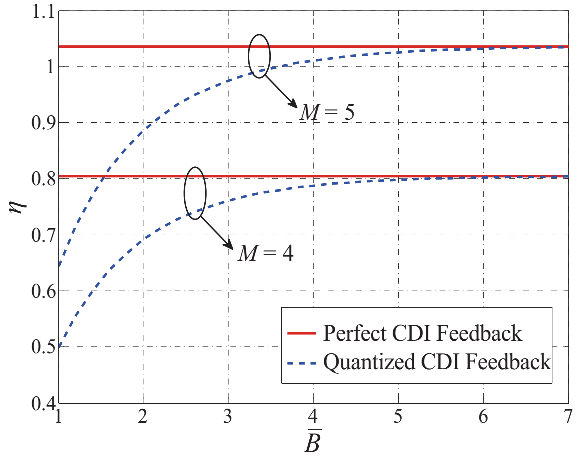

Fig. 3. Secrecy throughput versus $\bar{B}$ for $\rho_b = 3$ dB, $\rho_e = 0$ dB, $\bar{T} = 5$ and $\epsilon = \delta = 0.1$.

To examine the secrecy throughput loss caused by the limited feedback, Fig. 3 plots the secrecy throughput versus $\bar{B}$ with different values of M for two scenarios, namely, perfect CDI feedback and quantized CDI feedback. We clarify that $\bar{B} = B/M$ is the normalized feedback bits, which can be treated as the number of feedback bits used for each transmit antenna at Alice. We first observe that for a given M, the performance loss becomes smaller when $\bar{B}$ increases. This is not surprising since increasing feedback bits provides more perfect CDI available at Alice. We then observe that to for a fixed $\overline{B}$, increasing the number of transmit antennas leads to a greater performance loss. For example, when $M = 4$, $\overline{B} = 5$ is sufficient to achieve the secrecy throughput attainable with perfect CDI feedback. When $M = 5$, $\overline{B} = 6$ is required to achieve the same performance. This observation indicates that when M increases, more feedback bits for each antenna are needed.

VI. Conclusions

In this paper, we studied the design of secure transmission scheme in MISOSE scenario by explicitly taking account of the training and feedback overhead. Conditioned on the partial channel knowledge to the legitimate receiver and the statistical channel knowledge to the eavesdropper, we designed an on-off-based secure beamforming transmission scheme under dual outage constraints. We highlighted that this designed scheme is suitable for the deployment of physical layer security in practical communication systems.

Acknowledgement

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

Appendix A
Derivation of $f_{v\hat{\gamma}_b}(x)$ in (27)

Since v and $\hat{\gamma}_b$ are independent, the CDF of $v\hat{\gamma}_b$ can be formulated as [7]

$$\begin{aligned} F_{v\hat{\gamma}_b}(x) &= \Pr\{v\hat{\gamma}_b \le x\} = \int_0^\infty F_v\left(\frac{x}{y}\right) f_{\hat{\gamma}_b}(y)\,dy \\ &= \int_0^x f_{\hat{\gamma}_b}(y)\,dy + \int_x^{\frac{x}{1-\varepsilon}} \left(1 - N\left(1 - \frac{x}{y}\right)^{M-1}\right) f_{\hat{\gamma}_b}(y)\,dy \\ &= \int_0^{\frac{x}{1-\varepsilon}} f_{\hat{\gamma}_b}(y)\,dy - N\Omega = F_{\hat{\gamma}_b}\left(\frac{x}{1-\varepsilon}\right) - N\Omega, \end{aligned} \tag{35}$$

where Ω is derived as

$$\begin{aligned} \Omega &= \int_x^{\frac{x}{1-\varepsilon}} \left(1 - \frac{x}{y}\right)^{M-1} f_{\hat{\gamma}_b}(y)\,dy \\ &= \int_x^{\frac{x}{1-\varepsilon}} \left(1 - \frac{x}{y}\right)^{M-1} \frac{y^{M-1}}{\Gamma(M)\,\alpha_b^M} \exp\left(-\frac{y}{\alpha_b}\right) dy \\ &= \exp\left(-\frac{x}{\alpha_b}\right) \int_x^{\frac{x}{1-\varepsilon}} \frac{(y-x)^{M-1}}{\Gamma(M)\,\alpha_b^M} \exp\left(-\frac{y-x}{\alpha_b}\right) dy \\ &= \exp\left(-\frac{x}{\alpha_b}\right) F_{\hat{\gamma}_b}\left(\frac{\varepsilon x}{1-\varepsilon}\right). \end{aligned} \tag{36}$$

Thus we have

$$F_{v\hat{\gamma}_b}(x) = F_{\hat{\gamma}_b}\left(\frac{x}{1-\varepsilon}\right) - N\exp\left(-\frac{x}{\alpha_b}\right) F_{\hat{\gamma}_b}\left(\frac{\varepsilon x}{1-\varepsilon}\right). \tag{37}$$

Substituting (10) into (37), we have

$$\begin{aligned} F_{v\hat{\gamma}_b}(x) =& 1 - N\exp\left(-\frac{x}{\alpha_b}\right) - \exp\left(-\frac{x}{(1-\varepsilon)\,\alpha_b}\right) \\ & \times \sum_{m=0}^{M-1} \frac{1 - N\varepsilon^m}{\Gamma(m+1)} \left(\frac{x}{(1-\varepsilon)\,\alpha_b}\right)^m. \end{aligned} \tag{38}$$

By deriving the first order derivative of (38), we obtain the closed-form expression for $f_{v\hat{\gamma}_b}(x)$ as (27).

References

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

[2] T. Y. Liu, P. H. Lin, S. C. Lin, Y. W. P. Hong, and E. A. Jorswieck, “To avoid or not to avoid CSI leakage in physical layer secret communication system,” *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 19–25, Dec. 2015.

[3] 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.

[4] 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.

[5] 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.

[6] H. Wang, C. Wang, and W. Ng, “Artificial noise assisted secure transmission under training and feedback,” *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[7] W. Spantipach and M. L. Honig, “Optimization of training and feedback overhead for beamforming over block fading channels,” *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6103–6115, Dec. 2010.

[8] Z. Rezki, A. Khisti, and M. S. Alouini, “Ergodic secret message capacity of the wiretap channel with finite-rate feedback,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3364–3379, June 2014.

[9] T. Yoo, N. Jindal, and A. Goldsmith, “Multi-antenna downlink channels with limited feedback and user selection,” *IEEE J. Select. Areas Commun.*, vol. 25, no. 7, pp. 1478–1491, Sep. 2007.

[10] K. K. Mukkavilli, A. Sabharwal, E. Erkip, and B. Aazhang, “On beamforming with finite rate feedback in multiple-antenna systems,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2562–2579, Oct. 2003.

[11] D. J. Love, R. W. Heath, Jr., and T. Strohmer, “Grassmannian beamforming for multiple-input multiple-output wireless systems,” *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[12] M. Bloch, J. Barros, M. R. D. Rodriǵues, and S. M. McLauǵhlin, “Wireless information-theoretic security,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

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

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

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

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