Secrecy Capacity for Full-Duplex Massive MIMO Relaying Systems With Low-Resolution ADCs

Bridget Durowaa Antwi-Boasiako and Kyoung-Jae Lee
Department of Electronics and Control Engineering, Hanbat National University,
125 Dongseo-daero, Yuseong-gu, Daejeon, Korea
Emails: brigantwi@gmail.com, kyoungjae@hanbat.ac.kr

***Abstract*—In this paper, we consider an amplify-and-forward (AF) full duplex (FD) massive-antenna relay (or base station) aiding communication between K single-antenna source and destination pairs whose transmissions are overheard by one single-antenna eavesdropper. Maximum ratio combining (MRC) and maximum ratio transmission (MRT) processing is employed at the relay. The secrecy performance of the system is then derived with both relay and destination being equipped with low resolution analog-to-digital converters (ADCs). The results show the detrimental effect of the eavesdropper's presence on the sum rate of the system.**

I. Introduction

Fifth generation (5G) communication systems are gaining lots of traction in recent years. 5G promises very high data rate, low latency and provides support for many devices. 5G will incorporate full duplex (FD) systems, where transmission and reception of data is done simultaneously to theoretically double the spectral efficiency. Also technologies like massive MIMO, where many antennas are deployed at the base station to serve users, will be used to further enhance the 5G system performance. The issue of high hardware cost and power consumption could be curbed by using analog-to-digital converters (ADCs) with low resolution. The peformance loss due to quantization in low ADCs can be compensated for by the large number of antennas employed [1].

Wireless communication requires secured links to prevent interception of signals. FD systems could help improve secrecy and also the use of large scale antennas in massive MIMO systems allows simple beamforming techniques to be applied to enhance secrecy [2]. It has also been shown that the amplify-and-forward (AF) relaying scheme could achieve better security performance [3].

The main contribution of this paper is to derive the closed-form ergodic secrecy rate by employing MRC/MRT beamforming technique at the AF massive antenna relay in order to study the effect of the eavesdropper presence on the system rate.

II. System Model

Figure 1 considers a massive MIMO AF relaying system, where a FD relay (R) with M-massive receive and transmit antennas helps K single antenna-pair users (S_k, D_k) communicate, while an eavesdropper (E) tries to intercept the transmission between R and the destination (D).

Signal $\sqrt{p_s}x_{s,k}[i]$ is transmitted from each source S_k to R in the i-th time slot. The previously received signal

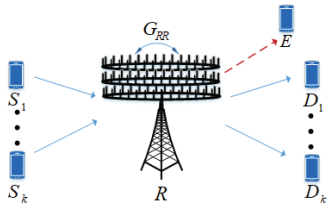

Fig. 1. FD massive MIMO AF relaying model with eavesdropper

$\tilde{\mathbf{y}}_R$ at R is processed with a linear processing matrix $\mathbf{F}$ and amplified to give signal $\mathbf{x}_R$. The relay then forwards $\mathbf{x}_R$ to D. E tries to eavesdrop on transmission between R and D. The signals received at R (after some form of self-interference mitigation), D and E are respectively expressed as

$$\mathbf{y}_R[i] = \sqrt{P_s}\mathbf{G}_{SR}\mathbf{x}_S[i] + \mathbf{G}_{RR}\hat{\mathbf{x}}_R[i] + \mathbf{n}_R[i], \quad (1)$$

$$\mathbf{y}_D[i] = \mathbf{G}_{RD}^T\mathbf{x}_R[i] + \mathbf{n}_D[i], \quad (2)$$

$$y_E[i] = \mathbf{g}_{RE}^T\mathbf{x}_R[i] + n_E[i], \quad (3)$$

where $\mathbf{G}_{SR} \in \mathbb{C}^{M\times K}$ with kth column $\mathbf{g}_{SR,k} \sim \mathcal{CN}(0, \beta_{SR,k}\mathbf{I}_M)$ and $\mathbf{G}_{RD} \in \mathbb{C}^{M\times K}$ with k-th column $\mathbf{g}_{RD,k} \sim \mathcal{CN}(0, \beta_{RD,k}\mathbf{I}_M)$ are channels from S to R and from R to D respectively.

$$\mathbf{g}_{\star,k} = \hat{\mathbf{g}}_{\star,k} + \mathbf{e}_{\star,k}, \quad (4)$$

$\hat{\mathbf{g}}_{\star,k}$ has variance $\sigma_{\star,k} = \dfrac{\alpha\tau_p p_p \beta_{\star,k}^2}{1+\tau_p p_p \beta_{\star,k}}$ and $\mathbf{e}_{\star,k}$ has variance $\tilde{\sigma}_{\star,k} = \dfrac{\beta_{\star,k} + (1-\alpha)\tau_p p_p \beta_{\star,k}^2}{1+\tau_p p_p \beta_{\star,k}}$, and $\star \in (SR, RD)$. The eavesdropper channel is given by $\mathbf{g}_{RE} \in \mathbb{C}^{M\times 1} \sim \mathcal{CN}(0, \beta_{RE}\mathbf{I}_M)$. $\bar{\mathbf{G}}_{RR} \in \mathbb{C}^{M\times M}$ is the loop interference channel, $\mathbf{n}_R[i]$, $\mathbf{n}_D[i]$ and $n_E[i]$ denote the noise at R, D, and E respectively and are i.i.d. $\mathcal{CN}(0,1)$. $\mathbf{x}_R[i] = \gamma\mathbf{F}\tilde{\mathbf{y}}_R[i-d]$ with γ being the amplification constant and MRC/MRT processing matrix $\mathbf{F} = \hat{\mathbf{G}}_{RD}^*\hat{\mathbf{G}}_{SR}^H$. $\mathbb{E}\{\hat{\mathbf{x}}_R[i]\hat{\mathbf{x}}_R^H[i]\} = \frac{PR}{M}\mathbf{I}_M$.

Because low ADCs are used at both R and D, the quantized versions of the signals at the receivers of R and D_k with linear gain α and distortion factor θ are given by

$$\tilde{\mathbf{y}}_R[i] = \alpha\mathbf{y}_R[i] + \tilde{\mathbf{n}}_R[i], \quad (5)$$

$$\tilde{y}_{D,k}[i] = \theta\mathbf{y}_{D,k}[i] + \tilde{\mathbf{n}}_{D,k}[i], \quad (6)$$

where $\tilde{\mathbf{n}}_R[i]$ and $\tilde{\mathbf{n}}_{D,k}[i]$ denote quantized versions of the noise at R and D_k respectively with covariance given by

$$\mathbf{R}_{\tilde{\mathbf{n}}_R[i]} = \alpha(1-\alpha)\text{diag}\left(\text{E}\left\{\mathbf{y}_R[i]\mathbf{y}_R[i]^H\right\}\right), \quad (7)$$

$$R_{\tilde{n}_{D,k}[i]} = \theta(1-\theta)\text{diagE}\left\{|y_{D,k}[i]|^2\right\}. \quad (8)$$

III. Secrecy Rate Analysis

Assuming D_k only has statistical knowledge of the channel, the received signal is expressed as in [1].

$$\tilde{y}_{D,k}[i] = \alpha\theta\gamma\sqrt{p_S}\text{E}\left\{\mathbf{g}_{RD,k}^T\mathbf{F}\mathbf{g}_{SR,k}\right\}x_{S,k}[i-d] + \underbrace{n_k^{eff}[i]}_{\text{effective noise}} \quad (9)$$

$$\begin{aligned} n_k^{eff}[i] &= \alpha\theta\gamma\sqrt{p_S}\left(\mathbf{g}_{RD,k}^T\mathbf{F}\mathbf{g}_{SR,k} - \text{E}\left\{\mathbf{g}_{RD,k}^T\mathbf{F}\mathbf{g}_{SR,k}\right\}\right)x_{S,k}[i-d] \\ &+ \underbrace{\alpha\theta\gamma\sqrt{p_S}\sum_{j\neq k}\mathbf{g}_{RD,k}^T\mathbf{F}\mathbf{g}_{SR,j}x_{S,j}[i-d]}_{\text{interpair interference}} \\ &+ \underbrace{\alpha\theta\gamma\mathbf{g}_{RD,k}^T\mathbf{F}\mathbf{G}_{RR}\hat{\mathbf{x}}_R[i-d]}_{\text{loop interference}} + \underbrace{\alpha\theta\gamma\mathbf{g}_{RD,k}^T\mathbf{F}\mathbf{n}_R[i-d]}_{\text{noise at the relay}} \\ &+ \underbrace{\theta\gamma\mathbf{g}_{RD,k}^T\mathbf{F}\tilde{\mathbf{n}}_R[i-d]}_{\text{quantization noise at at R}_k} + \underbrace{\theta n_{D,k}[i]}_{\text{noise at D}_k} + \underbrace{\tilde{n}_{D,k}[i]}_{\text{quantization noise at D}_k}. \end{aligned} \quad (10)$$

Assuming E has perfect knowledge of its own channel, the received signal at E is given by

$$\begin{aligned} \tilde{y}_E[i] &= \alpha\theta\gamma\sqrt{p_S}\mathbf{g}_{RE}^T\mathbf{F}\mathbf{g}_{SR,k}x_{S,k}[i-d] \\ &+ \alpha\theta\gamma\sqrt{p_S}\sum_{j\neq k}\mathbf{g}_{RE}^T\mathbf{F}\mathbf{g}_{SR,j}x_{S,j}[i-d] \\ &+ \alpha\theta\gamma\mathbf{g}_{RE}^T\mathbf{F}\mathbf{G}_{RR}\hat{\mathbf{x}}_R[i-d] + \alpha\theta\gamma\mathbf{g}_{RE}^T\mathbf{F}\mathbf{n}_R[i-d] \\ &+ \theta\gamma\mathbf{g}_{RE}^T\mathbf{F}\tilde{\mathbf{n}}_R[i-d] + n_E[i], \end{aligned} \quad (11)$$

where the first terms of (9) and (11) are the desired signals and the remaining terms are effective noise components.

The secrecy rate of the k-th user in AF FD massive MIMO relaying with low ADCs can be expressed as

$$secR_k = [R_k - R_E]^+, \quad (12)$$

where $[x]^+ = max(x, 0)$, R_k is the rate at the destination D_k whose solution is given in [1] and R_E is the rate at the eavesdropper E.

$$R_E = \frac{\tau_c - 2\tau_p}{\tau_c}\log(1+\text{SINR}_E), \quad (13)$$

where we define

$$SINR_E = \frac{A_{eve}}{C_{eve} + D_{eve} + F_{eve} + G_{eve}}, \quad (14)$$

$$\begin{aligned} A_{eve} &= psM^3\beta_{RE}\sigma_{RDk}^2\sigma_{SRk}^4 \\ &+ psM^2\beta_{RE}\sigma_{RDk}^2\sigma_{SRk}^2\beta_{SRk}, \\ C_{eve} &= M^2\beta_{REk}\textstyle\sum_{j\neq k}^K\beta_{SRj}\sum_{n\neq k,j}^K\sigma_{RDn}^2\sigma_{SRn}^2, \\ &+ M^2\beta_{REk}\sigma_{RDk}^2\sigma_{SRk}^2\textstyle\sum_{j\neq k}^K\beta_{SRj} \\ &+ M^3\beta_{REk}\textstyle\sum_{j\neq k}^K\sigma_{RDj}^2\sigma_{SRj}^4 \\ &+ M^2\beta_{REk}\textstyle\sum_{j\neq k}^K\sigma_{RDj}^2\sigma_{SRj}^2\beta_{SRj}, \\ D_{eve} &= p_RM^2(\sigma_{LI}^2+1)\beta_{RE}\textstyle\sum_{j=1}^K\sigma_{RDj}^2\sigma_{SRj}^2, \\ F_{eve} &= \tfrac{1-\alpha}{\alpha}(M^2\beta_{RE}\textstyle\sum_{n=1}^K\sigma_{RDn}^2\sigma_{SRn}^2, \\ &\times[\sigma_{SRn}^2 + \textstyle\sum_{i=1}^K\beta_{SR,i}] \\ &+ M^2\beta_{RE}(pR\sigma_{LI}^2+1)\textstyle\sum_{n=1}^K\sigma_{RDn}^2\sigma_{SRn}^2). \end{aligned}$$

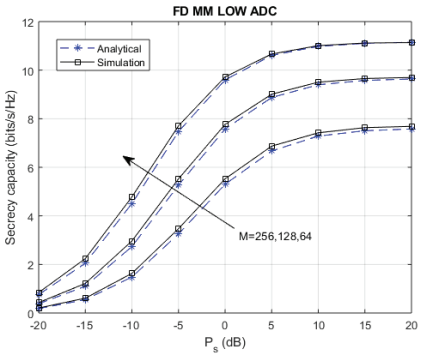

Fig. 2. Simulation vs analytic secrecy rate

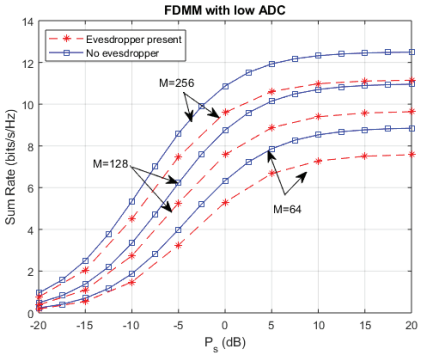

Fig. 3. Sumrate vs power

IV. Numerical Results

In this section, we confirm the results derived above by setting the coherence interval $\tau_c = 196$ symbols, $K = 5, \tau_p = K, \beta_{SR,k} = \beta_{RD,k} = \beta_{RE} = 1$, and $\sigma_{n_R}^2 = \sigma_{n_D}^2 = 1, \sigma_{LI}^2 = 0dB$, and $ps = p_R = p_p = 10dB$, $\theta = \alpha = 0.8825$. Figure 2 compares the result in (12) with the Monte-Carlo simulation result. Both results match tightly as the number of antennas increase, thus confirming our results.

The secrecy sum rate is then plotted against the sum rate in [1]. Figure 3 shows that the presence of the eavesdropper caused a decrease in sum rate as expected which has to be investigated and be further improved.

References

[1] C. Kong, C. Zhong, S. Jin, S. Yang, H. Lin, and Z. Zhang, "Full-duplex massive MIMO relaying systems with low-resolution adcs," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 5033–5047, Aug. 2017.

[2] J. Chen, X. Chen, W. H. Gerstacker, and D. W. K. Ng, "Resource allocation for a massive MIMO relay aided secure communication," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1700–1711, Aug. 2016.

[3] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: Af or df?," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 5135–5146, Sept. 2015.