MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Secrecy Performance of Finite-Sized Cooperative Full-Duplex Relay Systems with Unreliable Backhauls

Liu, H.; Kim, K.J.; Tsiftsis, T.A.; Kwak, K.S.; Poor, H.V.

TR2017-195 August 2017

Abstract

This paper investigates secrecy performance of finite-sized cooperative full-duplex relay (FDR) systems with unreliable wireless backhaul connections across multiple transmitters under Nakagami-m fading. Closed-form expressions for the secrecy outage probability and probability of non-zero achievable secrecy rate are derived in terms of self interference (SI), transmitter cooperation, and backhaul reliability. It is shown that transmitter cooperation can effectively enhance the secrecy performance, while the asymptotic limits on the secrecy outage probability and probability of non-zero achievable secrecy rate are exclusively determined by backhaul reliability. With the aid of transmitter cooperation, the burden of SI cancellation can be alleviated for the FDR system in achieving the allowed smallest secrecy outage probability. Compared to that of a half-duplex relay (HDR) system, the FDR system achieves a lower secrecy outage probability with well suppressed SI. The analysis shows that the secrecy outage probability achieved by the FDR system converges to that of the HDR system under perfect backhaul as the target secrecy rate becomes small. The secrecy performance metrics of the considered system are verified by simulations for various backhaul scenarios.

IEEE Transactions on Signal Processing

Secrecy Performance of Finite-Sized Cooperative Full-Duplex Relay Systems with Unreliable Backhauls

Hongwu Liu, *Member, IEEE,* Kyeong Jin Kim, *Senior Member, IEEE,*
Theodoros A. Tsiftsis, *Senior Member, IEEE,* Kyung Sup Kwak, *Member, IEEE,*
and H. Vincent Poor *Fellow, IEEE*

***Abstract*—This paper investigates secrecy performance of finite-sized cooperative full-duplex relay (FDR) systems with unreliable wireless backhaul connections across multiple transmitters under Nakagami-m fading. Closed-form expressions for the secrecy outage probability and probability of non-zero achievable secrecy rate are derived in terms of self interference (SI), transmitter cooperation, and backhaul reliability. It is shown that transmitter cooperation can effectively enhance the secrecy performance, while the asymptotic limits on the secrecy outage probability and probability of non-zero achievable secrecy rate are exclusively determined by backhaul reliability. With the aid of transmitter cooperation, the burden of SI cancellation can be alleviated for the FDR system in achieving the allowed smallest secrecy outage probability. Compared to that of a half-duplex relay (HDR) system, the FDR system achieves a lower secrecy outage probability with well suppressed SI. The analysis shows that the secrecy outage probability achieved by the FDR system converges to that of the HDR system under perfect backhaul as the target secrecy rate becomes small. The secrecy performance metrics of the considered system are verified by simulations for various backhaul scenarios.**

***Index Terms*—Wireless backhaul, full-duplex relay, two-hop relaying protocol, secrecy outage probability.**

I. Introduction

With the explosive demand for wireless data traffic, cooperative transmission is considered as a promising technology for future wireless communications. In particular, highly dense heterogeneous networks (HetNets) have attracted significant attentions, in which a mass of base stations or access points are deployed cooperatively to enhance user experience [1], [2]. However, with the dense deployment of cooperative nodes in HetNets, backhaul connections become increasingly worrisome [3], [4]. Although conventional wired backhauls provide solid link connections between the core network and control units (CUs) (such as access point or gateway), the associated capital expenses and operation expenses restrict their implementation. As an alternative solution to overcome inconvenience and excessive cost caused by wired backhauls, wireless backhauls have gained considerable interest [5], [6]. Due to wireless channel impairments such as non-line-of-sight (nLOS) propagation, severe fading, and interference, wireless backhauls are sometimes unreliable causing a serious issue in meeting end terminals' quality of service (QoS) requirements [7], [8].

A. Technical Literature Review

The reliability and limited-rate of wireless backhauls have been investigated for coordinated multi-point cooperation [9], cloud radio access networks [10], and finite-sized systems [11]. Considering backhaul link failures, the authors in [12] have derived upper and lower bounds on the achievable average rate for cooperative multi-relay systems. The rate-distortion region and outer bound on the rate region were investigated for relay backhauls with link erasures in [13] and limited-rate relay backhauls in [14], respectively. In [15], it was shown that wireless backhauls provided low latency multihop connections for multiple access points. For uplink backhaul connections, several cooperative relaying schemes have been proposed, including complex field network precoding [16], distributed compression [17], and decentralized decoding [18]. However, the existing works for cooperative relay systems with unreliable backhauls have considered only half-duplex relays (HDRs) at the price of 50% loss in spectral efficiency, which results from transmitting and receiving in orthogonal channels.

With their capability of transmitting and receiving signals simultaneously, full-duplex relays (FDRs) have attracted considerable recent attention [19], [20]. In [21] and [22], relay selection has been proposed to decrease the outage probability of FDR systems. In [23], several precoding/decoding, antenna selection, and power allocation techniques have been applied to maximize the end-to-end system performance of multiple-input multiple-output (MIMO) FDR systems. Due to self interference (SI) that leaks between transmit and receive antennas, FDR was previously considered impractical. Although recent advances in SI cancellation have shown that overall SI attenuation levels can be 70-100 dB, residual SI (RSI) cannot be eliminated completely due to RF impairments [24],

Manuscript received March 20, 2017; revised May 21, 2017; accepted August 16, 2017. The editor coordinating the review of this paper and approving it for publication was Prof. S. Tomasin.

H. Liu and K. S. Kwak are with the Department of Information and Communication Engineering, Inha University, Incheon, South Korea. H. Liu is also with Shandong Jiaotong University, Jinan 250357, China. (e-mail: hong.w.liu@hotmail.com)

K. J. Kim is with Mitsubishi Electric Research Laboratories, Cambridge, MA 02139 USA.

T. A. Tsiftsis is with the School of Engineering, Nazarbayev University, Astana, Kazakhstan.

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA.

[25]. Thus, system performance of FDR networks still suffers from RSI. To achieve substantially high spectral efficiency, SI cancellation and the corresponding RSI level need to be carefully handled [24], [25].

Due to the broadcast nature of wireless communications, potential receiver may receive signals intended for a legitimate receiver, so that data confidentiality in the legitimate channel can be compromised. Physical layer security, based on Shannon theory, and using channel coding to achieve secure transmission, is an emerging means of securing wireless transmissions against eavesdropping by exploiting physical channel characteristics [26], [27]. Several works have considered physical layer security over wireless relay channels, including distributed beamforming schemes [28], cooperative relay networks [29], buffer-aided relay networks [30], and MIMO communications [31]. It has been shown that the secrecy capacity of MIMO wiretap channels can be achieved by using Gaussian wiretap codes [32], [33], while multiple-antenna diversity has been analyzed for several transmit antenna selection (TAS) schemes in [34]–[36]. When a massive MIMO array is employed for relaying, significant enhancement of secrecy outage capacity can be achieved [37]. For simultaneous wireless information and power transfer (SWIPT) MIMO wiretap channels, the ergodic secrecy capacity has been approximated using large-dimensional random matrix theory [38]. In [39], the effects of unreliable backhaul on physical layer security of finite-sized cooperative HDR networks with multiple eavesdroppers were investigated. It has been shown that, compared to HDR systems, FDR systems can effectively decrease secrecy outage probability [40] and increase secrecy rate [41]. In [42], the secrecy performance of a multi-hop relay network was enhanced by employing an FDR. However, the effect of unreliable backhaul on physical layer security of finite-sized cooperative FDR systems remains unknown.

B. Motivation

In this paper, we explore physical layer security for a finite-sized cooperative FDR system, in which multiple transmitters are connected to a CU with unreliable backhaul and intend to transmit information to a destination via an intermediate FDR node. Different from TAS schemes designed for enhancing physical layer security [34]–[36], where transmit antennas are co-located at a single source node, the considered transmitter cooperation is deployed with unreliable wireless backhaul, which serves as a relaying-hop from the CU to transmitters. Intuitively, when perfect wireless backhaul across all transmitters is available, the considered transmitter cooperation can be recognized as a multiple-antenna source node with TAS. Moreover, unlike the works in [40] and [41], in which FDR-assisted jamming was employed, we considered a simple but insightful scenario in which a single transmitter is selected for transmitting to the destination [39], while an eavesdropper can overhear any confidential messages transmitted by the selected transmitter and FDR node.

C. Our Contributions

- The secrecy outage probability and probability of non-zero achievable secrecy rate are derived for a finite-sized cooperative FDR system with respect to RSI, transmitter cooperation, and backhaul reliability. Note that an investigation of the joint impact of RSI, transmitter cooperation, and backhaul reliability in cooperative relay systems has not been investigated previously. Thus, its accompanying secrecy performance analysis is also a novel contribution from this work. For finite-sized cooperative FDR systems, we consider Nakagami-m fading channels which are fairly general, modeling a range of fading behaviors.
- Closed-form expressions for the secrecy outage probability and probability of non-zero achievable secrecy rate are derived for a finite-sized cooperative HDR system, which serves as a benchmark for secrecy performance comparison between HDR and FDR systems.
- Asymptotic limits of the secrecy outage probability and probability of non-zero achievable secrecy rate are obtained for both HDR and FDR systems, including an intrinsic outage probability floor and a ceiling on the probability of non-zero achievable secrecy rate. For the FDR system, it is verified that the asymptotic limits can be achieved only when SI is well suppressed.

The remainder of this paper is organized as follows: Section II presents the system model and the statistical properties of the signal-to-interference-plus-noise ratios (SINRs); Section III analyzes the secrecy performance of the FDR system; Section IV analyzes the secrecy performance of the HDR system; Section V gives simulation results to verify the analysis, and Section VI summarizes the paper.

Notation: $\mathbb{E}(\cdot)$ denotes the expectation and $\mathcal{CN}(x, y)$ stands for the circularly symmetric complex Gaussian distribution with the mean x and variance y. $\mathbf{0}_{M\times N}$ is the $M\times N$ zero matrix and $\mathbf{I}_N$ is the $N\times N$ identity matrix. $U(\cdot)$ denotes the unit step function. $\Gamma(\cdot)$ is the gamma function. $[x]^+ \triangleq \max(0, x)$ and Z^+ is the set of positive integers. $f_\varphi(\cdot)$, $F_\varphi(\cdot)$, and $\bar{F}_\varphi(\cdot)$ denote the probability density function (PDF), cumulative distribution function (CDF), and complementary CDF (CCDF) of the random variable (RV) φ, respectively.

II. System and Channel Model

The considered finite-sized system consists of a CU providing wireless backhaul to K transmitters ($TX_1, \ldots, TX_K$) communicating with a destination D via an FDR node R in the presence of an eavesdropper E, as depicted in Fig. 1. Due to large path loss or obstacles, we assume that the direct links between the transmitters and destination do not exist. In addition, we assume that each transmitter is equipped with a single transmit antenna, the FDR node is equipped with a single receive and a single transmit antenna, while the destination and eavesdropper are each equipped with a single receive antenna.

A. Unreliable Backhaul

Backhaul reliability for the transmitter TX_k is denoted by s_k, which represents the probability that TX_k can successfully decode the source message via its backhaul transmission. In contrast, the probability that the transmitter TX_k cannot decode the source message via its dedicated backhaul is $1-s_k$.

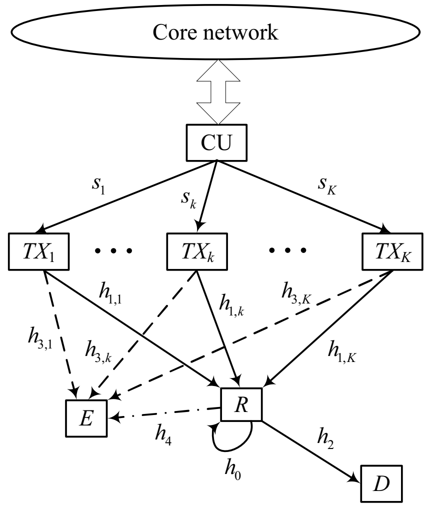

Fig. 1. Block diagram of a finite-sized cooperative FDR system with unreliable backhauls.

When a backhaul transmission is not successful, we do not apply automatic repeat request (ARQ) or power control, so that the corresponding transmitter may not have the correct information of the source message [43]. Backhaul reliability is assumed to be independent across source messages following a Bernoulli process [39], so that $\Pr(\mathbb{I}_k = 1) = s_k$ and $\Pr(\mathbb{I}_k = 0) = 1 - s_k$, where $\mathbb{I}_k$ is a binary indicator function.

B. Channel

The channels of the links $TX_k \rightarrow R$, $R \rightarrow D$, $TX_k \rightarrow E$, and $R \rightarrow E$ are denoted by $h_{1,k}$, h_2, $h_{3,k}$, and h_4, respectively. A path loss associated with h_i for $i \in \{(1,k), 2, (3,k), 4\}$ is denoted by $\mathcal{L}_i$ and the channel magnitude $|h_i|$ for $i \in \{(1,k), 2, (3,k), 4\}$ is modeled as Nakagami-m fading, so that $|h_i|^2$ follows the gamma distribution which is denoted by $|h_i|^2 \sim \mathrm{Ga}(m_i, \theta_i)$, where m_i is the shape factor and θ_i is the scale factor. For analytical analysis convenience, we limit to the case of Nakagami-m fading with a positive integer value of m. The SI channel at the relay is denoted by h_0. Before any active interference cancellation, the SI channel amplitude $|h_0|$ in the RF domain can be characterized as Rician [25]. In practice, the actual distribution of $|h_0|$ is not known after several stages of SI cancellation [44]. Therefore, this paper conducts the system modeling and secrecy performance analysis conditioned on RSI power level. All the channels are assumed to be super-block-fading, i.e., the channel coefficients remain constant, but independently vary from one super-block to another super-block. Similar to the existing works [37], [39], [40], [42], [45], we assume that the relay knows perfect channel state information (CSI) of the links $TX_k \rightarrow R$, the destination knows perfect CSI of the link $R \rightarrow D$, and the eavesdropper knows perfect CSI of the links $TX_k \rightarrow E$ and $R \rightarrow E$.

C. Cooperative Signal Processing

In the considered FDR transmission, the length of one super-block is denoted by $B + \tau$, where B is the number of blocks transmitted by the selected transmitter in each super-block and τ is the processing delay at the relay [46].

At the beginning of each super-block transmission, a transmitter with the strongest channel gain is selected to transmit to the relay [39], so that the selected transmitter index is given by

$$k^* = \arg\max_{1 \le k \le K} \mathbb{I}_k \mathcal{L}_{1,k} |h_{1,k}|^2. \tag{1}$$

After receiving the signal, the FDR node first decodes the source signal and regenerates it by assuming that the decode-and-forward (DF) relay protocol is employed [39]. Thus, we have $x_r(t) = x_s(t-\tau)$ at the tth block, where $x_s(t)$ and $x_r(t)$ are the transmission signals by the source and relay satisfying $\mathbb{E}(x_s(t)) = 1$ and $\mathbb{E}(x_r(t)) = 1$.

The received signal at the FDR node can be expressed as

$$\begin{aligned} y_r(t) &= \sqrt{P_s \mathcal{L}_{1,k^*}} h_{1,k^*} \mathbb{I}_{k^*} x_s(t) + \\ &\quad \sqrt{P_r} h_0 x_s(t-\tau) + z_r(t), \end{aligned} \tag{2}$$

where P_s is the allocated transmission power at the selected transmitter, P_r is the transmission power at the relay, and $z_r(t) \sim \mathcal{CN}(0, \sigma^2)$ is the additive white Gaussian noise. Moreover, the received signal at the destination can be expressed as

$$y_d(t) = \sqrt{P_r \mathcal{L}_2} h_2 x_s(t-\tau) + z_d(t), \tag{3}$$

where $z_d(t) \sim \mathcal{CN}(0, \sigma^2)$ is the additive white Gaussian noise at the destination. Because the selected transmitter and relay transmit simultaneously, the intercepted signal at the eavesdropper is given by

$$\begin{aligned} y_e(t) &= \sqrt{P_s \mathcal{L}_{3,k^*}} h_{3,k^*} \mathbb{I}_{k^*} x_s(t) + \\ &\quad \sqrt{P_r \mathcal{L}_4} h_4 x_s(t-\tau) + z_e(t). \end{aligned} \tag{4}$$

With the super-block structure, the intercepted signal can be rewritten in a matrix form as

$$\boldsymbol{y}_e = \boldsymbol{H} \boldsymbol{x}_s + \boldsymbol{z}_e(t), \tag{5}$$

where $\boldsymbol{y}_e = [y_e(B+\tau+t-1), y_e(B+\tau+t-2), \ldots, y_e(t)]^T$, $\boldsymbol{x}_s = [x_s(B+t-1), x_s(B+t-2), \ldots, x_s(t)]^T$, $\boldsymbol{z}_e = [z_e(B+\tau+t-1), z_e(B+\tau+t-2), \ldots, z_e(t)]^T$, and

$$\begin{aligned} \boldsymbol{H} = & \sqrt{P_s \mathcal{L}_{3,k^*}} h_{3,k^*} \mathbb{I}_{k^*} \begin{bmatrix} \boldsymbol{I}_B \\ \boldsymbol{0}_{\tau \times B} \end{bmatrix} + \\ & \sqrt{P_r \mathcal{L}_4} h_4 \begin{bmatrix} \boldsymbol{0}_{\tau \times B} \\ \boldsymbol{I}_B \end{bmatrix} \end{aligned} \tag{6}$$

is the $(B+\tau) \times B$ eavesdropping channel matrix.

III. Derivation of the SINRs and SNR

According to (2)-(3), the SINR at the relay and the signal-to-noise ratio (SNR) at the destination are respectively given by

$$\gamma_r \triangleq \frac{\mathbb{I}_{k^*} P_s \mathcal{L}_{1,k^*} |h_{1,k^*}|^2}{P_r |h_0|^2 + \sigma^2} \approx \frac{\mathbb{I}_{k^*} P_s \mathcal{L}_{1,k^*} |h_{1,k^*}|^2 / \sigma^2}{\gamma_{\mathrm{RSI}}} \text{ and} \tag{7}$$

$$\gamma_d \triangleq \frac{P_r \mathcal{L}_2 |h_2|^2}{\sigma^2}, \tag{8}$$

where $\gamma_{\rm RSI} \triangleq P_r|h_0|^2/\sigma^2$ is the interference-to-noise ratio (INR) at the relay. Note that the RSI power is $P_r|h_0|^2$ since we use h_0 to model the SI channel after a series of interference cancellations. In (7), the approximation is achieved in the interference-dominated scenario which is of practical interest. With the above obtained γ_r and γ_d, the end-to-end SINR of the main relaying channel is given by $\gamma_{\rm FDR} = \min(\gamma_r, \gamma_d)$ [39]. Since (5) has a similar form as that of the inter-symbol interference channels, the B eigenvalues of $\boldsymbol{H}^H\boldsymbol{H}$ can be derived as [46]

$$\lambda_{\tau(i-1)+1:\tau i} \triangleq P_s\mathcal{L}_{3,k^*}|h_{3,k^*}|^2\mathbb{I}_{k^*} + P_r\mathcal{L}_4|h_4|^2 + 2P_sP_r\mathcal{L}_{3,k^*}\mathcal{L}_4|h_{3,k^*}^*h_4|\cos\frac{i\tau\pi}{\tilde{B}+\tau}, \quad (9)$$

where $i \in \{1,2,\ldots,n\}$ with $n \in Z^+$, $\tilde{B} = n\tau$, and $\lambda_{i:j}$ denotes the set $\{\lambda_i, \lambda_{i+1}, \ldots, \lambda_j\}$. From (9), the ith ($i = 1,2,\ldots,B$) equivalent SINR with respect to (5) can be effectively approximated as [46]

$$\gamma_i = \frac{\lambda_i}{\sigma^2} \approx \gamma_e \triangleq \frac{P_s\mathcal{L}_{3,k^*}|h_{3,k^*}|^2\mathbb{I}_{k^*} + P_r\mathcal{L}_4|h_4|^2}{\sigma^2}, \quad (10)$$

which makes the performance metric utilizing γ_i independent of the super-block parameters B and τ. In the following, we use the definitions $\tilde{\theta}_{1,k} \triangleq \frac{P_s\mathcal{L}_{1,k}\theta_{1,k}}{P_r|h_0|^2}$, $\tilde{\theta}_2 \triangleq \frac{P_r\mathcal{L}_2\theta_2}{\sigma^2}$, $\breve{\theta}_1 \triangleq \frac{P_s\mathcal{L}_{3,k^*}\theta_{3,k^*}}{\sigma^2}$, and $\breve{\theta}_2 \triangleq \frac{P_r\mathcal{L}_4\theta_4}{\sigma^2}$.

A. Statistical Properties of the SINRs

Conditioned on the RSI power level, the RV γ_r can be recognized as the largest of K products of gamma RVs and Bernoulli random RVs. Based on the theory of the order statistics, the following proposition is provided for the CDF of γ_r.

Proposition 1. *The CDF of the SINR γ_r is given by*

$$F_{\gamma_r}(x) = 1 + \sum_{k=1}^{K}\Upsilon(-1)^k\prod_{q=1}^{k}\left(\frac{s_{\ell_q}}{n_q!(\tilde{\theta}_{1,\ell_q})^{n_q}}\right)e^{-\alpha x}x^{\beta}, \quad (11)$$

where $\alpha \triangleq \sum_{q=1}^{k}\tilde{\theta}_{1,\ell_q}^{-1}$, $\beta \triangleq \sum_{q=1}^{k} n_q$, and

$$\Upsilon \triangleq \sum_{\ell_1=1}^{K-k+1}\sum_{\ell_2=\ell_1+1}^{K-k+2}\cdots\sum_{\ell_k=\ell_{k-1}+1}^{K}\sum_{n_1=0}^{m_{1,\ell_1}-1}\sum_{n_2=0}^{m_{1,\ell_2}-1}\cdots\sum_{n_k=0}^{m_{1,\ell_k}-1}. \quad (12)$$

Proof: See Appendix A. ■

The closed-form expression in (11) is of particular interest since it can be applied in a wide range scenarios with non-identical backhaul reliability, non-identical Nakagami-m fading channels, and any degree of transmitter cooperation. Moreover, since that $\tilde{\theta}_{1,\ell_q} = \frac{P_s\mathcal{L}_{1,\ell_q}\theta_{1,\ell_q}/\sigma^2}{\gamma_{\rm RSI}}$, the distribution of γ_r in (11) is explicitly conditioned on RSI, so that the impact of the FDR operation on γ_r can be analytically evaluated based on the expression in Proposition 1.

Theorem 1. *The CDF of the SINR of the cooperative FDR transmission with unreliable backhauls and transmitter cooperation is given by*

$$F_{\gamma_{\rm FDR}}(x) = 1 - \sum_{k=1}^{K}\Upsilon(-1)^{k+1}\prod_{q=1}^{k}\left(\frac{s_{\ell_q}}{n_q!(\tilde{\theta}_{1,\ell_q})^{n_q}}\right)\sum_{n=0}^{m_2-1}\frac{1}{n!(\tilde{\theta}_2)^n}e^{-x(\alpha+1/\tilde{\theta}_2)}x^{\beta+n}. \quad (13)$$

Proof: See Appendix B. ■

The closed-form expression in Theorem 1 explicitly considers transmitter cooperation, backhaul reliability, Nakagami-m fading, as well as RSI, so that it provides a general form for the end-to-end SINR distribution of the main relaying channel of the finite-sized cooperative FDR system. Moreover, the joint impact of the considered practical system setting on $\gamma_{\rm FDR}$ is characterized. Since $\tilde{\theta}_{1,\ell_q}$ includes RSI power level, the impact of RSI on $\gamma_{\rm FDR}$ can be readily evaluated based on (13).

To derive the PDF and CDF of γ_e, we introduce a gamma random variable $Z_{\mu,\nu} \sim {\rm Ga}(\nu, \breve{\theta}_\mu)$ with its PDF and CDF given by

$$f_{Z_{\mu,\nu}}(x) \triangleq \frac{x^{\nu-1}e^{-x/\breve{\theta}_\mu}}{\Gamma(\nu)(\breve{\theta}_\mu)^\nu} \quad (14)$$

and

$$F_{Z_{\mu,\nu}}(x) \triangleq 1 - e^{-x/\breve{\theta}_\mu}\sum_{\ell=0}^{\nu-1}\frac{1}{\ell!}\left(\frac{x}{\breve{\theta}_\mu}\right)^{\ell}, \quad (15)$$

respectively, where $\mu = 1,2$ and $\nu = 1,\ldots,\breve{m}_\mu$ with $\breve{m}_1 \triangleq m_{3,k^*}$ and $\breve{m}_2 \triangleq m_4$. Since transmitter k^* determined by (1) is randomly selected from a particular set of transmitters, the evaluation of the statistics of the SINR of the eavesdropping channel is only feasible by considering identical backhaul reliability and identical Nakagami-m fading for the channels $h_{3,k}$ but non-identical Nakagami-m fading channels for the $TX_k \to R$, $R \to D$, and $R \to E$ links. This assumption will be relaxed to non-identical backhaul reliability and non-identical Nakagami-m fading channels across all the links in the next section. Due to different locations of the transmitters, relay, and eavesdropper, we also assume $\breve{\theta}_1 \neq \breve{\theta}_2$.

Proposition 2. *The PDF and CDF of the SINR received by the eavesdropper are respectively given by*

$$f_{\gamma_e}(x) = (1-s_{k^*})f_{Z_{2,\breve{m}_2}}(x) + s_{k^*}\sum_{\mu=1}^{2}\sum_{\nu=1}^{\breve{m}_\mu}\Xi_{\mu,\nu}f_{Z_{\mu,\nu}}(x) \quad (16)$$

and

$$F_{\gamma_e}(x) = (1-s_{k^*})F_{Z_{2,\breve{m}_2}}(x) + s_{k^*}\sum_{\mu=1}^{2}\sum_{\nu=1}^{\breve{m}_\mu}\Xi_{\mu,\nu}F_{Z_{\mu,\nu}}(x), \quad (17)$$

where $\Xi_{\mu,\nu}$ is given by

$$\Xi_{\mu,\nu} \triangleq (-1)^{\breve{m}_1+\breve{m}_2-\breve{m}_\mu}\breve{\theta}_\mu^{\nu}(\breve{m}_1+\breve{m}_2-\nu-1)!\frac{\left(\frac{1}{\breve{\theta}_\mu} - \frac{1}{\breve{\theta}_{1+U(1-\mu)}}\right)^{\nu-\breve{m}_1-\breve{m}_2}}{\breve{\theta}_1^{\breve{m}_1}\breve{\theta}_2^{\breve{m}_2}(\breve{m}_{1+U(1-\mu)}-1)!(\breve{m}_\mu-\nu)!}. \quad (18)$$

Proof: See Appendix C. ■

The closed-form expressions in Proposition 2 explicitly include the impact of the simultaneous reception from both the transmitter and relay due to the FDR operation, while the backhaul reliability on the distribution of γ_e is also characterized.

IV. Secrecy Performance Analysis

Based on available closed-form expressions for the CDF and PDF of SINRs and SNR, this section computes the secrecy outage probability and probability of non-zero achievable secrecy rate for the finite-sized cooperative FDR system under non-identical Nakagami-m fading. With respect to the random transmitter selection from the point of view of the eavesdropper, we first evaluate the secrecy performance metrics with identical backhaul reliability and identical Nakagmai-m fading for the channels $h_{3,k}$. However, all the other links of the system are assumed following non-identical Nakagami-m fading. Then, we derive the asymptotic secrecy performance limits by considering non-identical backhaul reliability and non-identical Nakagami-m fading across all the links in the high SINR/SNR region.

For the main relaying channel, the achievable maximum rate of one realization of the super-block transmission is given by [46]

$$C_{\mathrm{FDR}} = \log_2(1+\gamma_{\mathrm{FDR}}), \tag{19}$$

while the achievable maximum rate for the eavesdropping channel can be expressed as [40]

$$\begin{aligned} C_e &= \frac{1}{B}\log_2\left(\det(\boldsymbol{I}_B + \boldsymbol{H}^H\boldsymbol{H})\right) \\ &= \frac{1}{B}\log_2\prod_{i=1}^{B}(1+\gamma_i). \end{aligned} \tag{20}$$

With the approximation provided in (10), (20) can be approximated as

$$C_e \approx \log_2(1+\gamma_e). \tag{21}$$

Since C_{FDR} and C_e are measured at the super-block level, we introduce $C_s = [C_{\mathrm{FDR}} - C_e]^+$ as the secrecy rate that can be achieved by the main relaying channel with a Gaussian wiretap code for one realization of the super-block transmission [40], [47]. Substituting (19) and (21) into $C_s = [C_{\mathrm{FDR}} - C_e]^+$, it can be shown

$$C_s = \left[\log_2(1+\gamma_{\mathrm{FDR}}) - \log_2(1+\gamma_e)\right]^+. \tag{22}$$

A. Identical Backhaul Reliability

For identical backhaul reliability, we investigate the secrecy performance next.

1) Secrecy Outage Probability: In [26], Shannon proved that perfect secrecy can be achieved by using a one-time pad if the entropy of the private key, used to encrypt the message, is larger than or equal to the entropy of the message itself. When the secrecy rate C_s is less than a target secrecy rate $R_s > 0$, perfect secrecy cannot be guaranteed and a secrecy outage event occurs [40], [47]. The secrecy outage probability can be characterized as [40], [47], [48]

$$\begin{aligned} P_{\mathrm{out}} &= \Pr(C_s < R_s) \\ &= \int_0^\infty F_{\gamma_{\mathrm{FDR}}}(J_{\mathrm{FDR}}(1+x)-1) f_{\gamma_e}(x)\mathrm{d}x, \end{aligned} \tag{23}$$

where $J_{\mathrm{FDR}} \triangleq 2^{R_s}$.

Theorem 2. *The secrecy outage probability of a finite-sized cooperative FDR system with identical backhaul but non-identical Nakagami-m fading is given by* (24) *at the next page.*

Proof: Substituting (13) and (16) into (23), we expand the term $(J_{\mathrm{FDR}} - 1 + J_{\mathrm{FDR}}x)^{\beta+n}$ in the obtained expression using the binomial formula. Then, by solving the resulted integral using $\int_0^\infty x^m e^{-ax^n}\mathrm{d}x = \Gamma((m+1)/n)/(na^{(m+1)/n})$ [49, 3.326/2], (24) can be arrived. ■

Theorem 2 provides an analytical framework for evaluation/design the secrecy outage probability of a finite-sized cooperative FDR system in terms of CSI statistics, transmitter cooperation, backhaul reliability, and RSI power level. Moreover, the closed-from expression in (24) considers that the eavesdropper simultaneously receives signals from both the transmitter and relay, which affects P_{out} with respect to the FDR operation besides RSI. Although the secrecy outage probability is a general secrecy performance metric, the derivations for (24) are novel since we consider a practical full-duplex system that faces RSI, unreliable backhaul, and transmitter cooperation under Nakagami-m fading, which has not been investigated previously.

2) Probability of Non-Zero Achievable Secrecy Rate: The probability of non-zero achievable secrecy rate is given by [47]

$$\Pr(C_s > 0) = \int_0^\infty \bar{F}_{\gamma_{\mathrm{FDR}}}(x) f_{\gamma_e}(x)\mathrm{d}x, \tag{25}$$

which is evaluated as (26) at the next page. Note that $\bar{F}_{\gamma_{\mathrm{FDR}}}(x) = 1 - F_{\gamma_{\mathrm{FDR}}}(x)$ can be extracted from (13).

3) Asymptotic Performance with Perfect Backhauls: Asymptotic secrecy outage probability and asymptotic probability of non-zero achievable rate with perfect backhauls are given by the following theorem.

Theorem 3. *For perfect backhaul connections and limited RSI, asymptotic secrecy outage probability and probability of non-zero achievable secrecy rate are given by Eqs.* (27) *and* (28) *at the next page. In Eqs.* (27) *and* (28), *we defined* $\tilde{m}_{1,k} \triangleq \sum_{k=1}^{K} m_{1,k}$.

Proof: See Appendix D. ■

The closed-form expressions in Theorem 3 clearly show that the asymptotic secrecy performance limits under perfect backhaul and limited RSI are determined by transmitter cooperation, Nakagami-m fading, and FDR operation. Moreover, Theorem 3 shows that the impact of full-duplex operation on the asymptotic secrecy performance limits comes from not only the simultaneous reception and transmission in the main relaying channel, but also the simultaneous receptions from the transmitter and relay in the eavesdropping channel. Note that a full-duplex system with RSI, unreliable backhaul, and transmitter cooperation has not been investigated previously,

$$P_{\rm out} = 1 - \sum_{k=1}^{K} \Upsilon (-1)^{k+1} \prod_{q=1}^{k} \left(\frac{s_{\ell_q}}{n_q! (\tilde{\theta}_{1,\ell_q})^{n_q}} \right) \sum_{n=0}^{m_2-1} \frac{1}{n! (\tilde{\theta}_2)^n} \sum_{i=0}^{\beta+n} \binom{\beta+n}{i} (J_{\rm FDR}-1)^{\beta+n-i} J_{\rm FDR}^{i}$$
$$e^{-(J_{\rm FDR}-1)(\alpha+1/\tilde{\theta}_2)} \left[\frac{(1-s_{k^*}) \Gamma(i+\breve{m}_2)}{\Gamma(\breve{m}_2) \breve{\theta}_2^{\breve{m}_2}} \left(J_{\rm FDR}\alpha + \frac{J_{\rm FDR}}{\tilde{\theta}_2} + \frac{1}{\breve{\theta}_2} \right)^{-(i+\breve{m}_2)} \right.$$
$$\left. + s_{k^*} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \frac{\Gamma(i+\nu)}{\Gamma(\nu) \breve{\theta}_\mu^{\nu}} \left(J_{\rm FDR}\alpha + \frac{J_{\rm FDR}}{\tilde{\theta}_2} + \frac{1}{\breve{\theta}_\mu} \right)^{-(i+\nu)} \right]. \quad (24)$$

$$\Pr(C_s > 0) = \sum_{k=1}^{K} \Upsilon (-1)^{k+1} \prod_{q=1}^{k} \left(\frac{s_{\ell_q}}{n_q! (\tilde{\theta}_{1,\ell_q})^{n_q}} \right) \sum_{n=0}^{m_2-1} \frac{1}{n! (\tilde{\theta}_2)^n}$$
$$\left[(1-s_{k^*}) \frac{\Gamma(\beta+n+\breve{m}_2)}{\Gamma(\breve{m}_2) \breve{\theta}_2^{\breve{m}_2}} \left(\alpha + \frac{1}{\tilde{\theta}_2} + \frac{1}{\breve{\theta}_2} \right)^{-(\beta+n+\breve{m}_2)} \right.$$
$$\left. + s_{k^*} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \frac{\Gamma(\beta+n+\nu)}{\Gamma(\nu) \breve{\theta}_\mu^{\nu}} \left(\alpha + \frac{1}{\tilde{\theta}_2} + \frac{1}{\breve{\theta}_\mu} \right)^{-(\beta+n+\nu)} \right]. \quad (26)$$

$$P_{\rm out}^{\rm as} = \begin{cases} \frac{\sum_{i=0}^{\tilde{m}_{1,k}} \binom{\tilde{m}_{1,k}}{i} (J_{\rm FDR}-1)^{\tilde{m}_{1,k}-i} J_{\rm FDR}^{i} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+i) (\breve{\theta}_\mu)^i / \Gamma(\nu)}{\prod_{k=1}^{K} m_{1,k}! (\tilde{\theta}_{1,k})^{m_{1,k}}}, & \text{when } m_2 > \tilde{m}_{1,k}, \\ \frac{\sum_{i=0}^{m_2} \binom{m_2}{i} (J_{\rm FDR}-1)^{m_2-i} J_{\rm FDR}^{i} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+i) (\breve{\theta}_\mu)^i / \Gamma(\nu)}{m_2! (\tilde{\theta}_2)^{m_2}}, & \text{when } m_2 < \tilde{m}_{1,k}, \\ \frac{\sum_{i=0}^{\tilde{m}_{1,k}} \binom{\tilde{m}_{1,k}}{i} (J_{\rm FDR}-1)^{\tilde{m}_{1,k}-i} J_{\rm FDR}^{i} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+i) (\breve{\theta}_\mu)^i / \Gamma(\nu)}{\prod_{k=1}^{K} m_{1,k}! (\tilde{\theta}_{1,k})^{m_{1,k}}} & \\ \quad + \frac{\sum_{i=0}^{m_2} \binom{m_2}{i} (J_{\rm FDR}-1)^{m_2-i} J_{\rm FDR}^{i} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+i) (\breve{\theta}_\mu)^i / \Gamma(\nu)}{m_2! (\tilde{\theta}_2)^{m_2}}, & \text{when } m_2 = \tilde{m}_{1,k}. \end{cases} \quad (27)$$

$$\Pr^{\rm as}(C_s > 0) = \begin{cases} 1 - \frac{\sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+\tilde{m}_{1,k}) (\breve{\theta}_\mu)^{\tilde{m}_{1,k}} / \Gamma(\nu)}{\prod_{k=1}^{K} m_{1,k}! (\tilde{\theta}_{1,k})^{m_{1,k}}}, & \text{when } m_2 > \tilde{m}_{1,k}, \\ 1 - \frac{\sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+\tilde{m}_{1,k}) (\breve{\theta}_\mu)^{\tilde{m}_{1,k}} / \Gamma(\nu)}{m_2! (\tilde{\theta}_2)^{m_2}}, & \text{when } m_2 < \tilde{m}_{1,k}, \\ 1 - \frac{\sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+\tilde{m}_{1,k}) (\breve{\theta}_\mu)^{\tilde{m}_{1,k}} / \Gamma(\nu)}{\prod_{k=1}^{K} m_{1,k}! (\tilde{\theta}_{1,k})^{m_{1,k}}} & \\ \quad - \frac{\sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \Gamma(\nu+\tilde{m}_{1,k}) (\breve{\theta}_\mu)^{\tilde{m}_{1,k}} / \Gamma(\nu)}{m_2! (\tilde{\theta}_2)^{m_2}}, & \text{when } m_2 = \tilde{m}_{1,k}. \end{cases} \quad (28)$$

and thus the results in Theorem 3 provide novel insight into the joint impact of the practical system setting on the asymptotic secrecy performance limits. According to the results of Theorem 3, the secrecy diversity gain can be defined as

$$D = \min\left(\sum\nolimits_{k=1}^{K} m_{1,k}, m_2 \right), \quad (29)$$

which indicates that the diversity gain is mainly determined by the shape factor of the Nakagami-m fading, whereas transmitter cooperation does not affect the secrecy diversity gain.

B. Asymptotic Analysis with Non-Identical Backhaul Reliability and Nakagami-m Fading

With well suppressed SI at the FDR node and fixed received SINR at the eavesdropper, unreliable backhauls result in the inevitable limits on the secrecy outage probability and probability of non-zero achievable secrecy rate, which are given by the following theorem.

Theorem 4. *At a fixed received SINR at the eavesdropper and with well suppressed SI at the FDR node, an asymptotic secrecy outage probability limit and an asymptotic limit on the probability of non-zero achievable secrecy rate are respectively given by*

$$P_{\rm out}^{as} = \prod_{k=1}^{K} (1 - s_k) \quad \textit{and} \quad (30)$$

$$\Pr^{as}(C_s > 0) = 1 - \prod_{k=1}^{K} (1 - s_k). \quad (31)$$

Proof: See Appendix E. ■

Theorem 4 shows that asymptotic limits on the secrecy outage probability and probability of non-zero achievable secrecy rate are exclusively determined by a set of backhaul reliability levels, $\{s_k\}$, which provides new insight into the considered full-duplex system. For a special case of the identical backhaul reliability $s_k = s$, $\forall k$, asymptotic limits can be written as $P_{\rm out}^{as,K} = (1-s)^K$ and $P_r^{as,K}(C_s > 0) = 1-(1-s)^K$. Furthermore, we have $P_{\rm out}^{as,K} \to 0$ and $P_r^{as,K}(C_s > 0) = 1$ as $s_k \to 1$. According to Theorem 4, as backhaul reliability increases, a lower secrecy outage occurs. For non-perfect backhaul connections, Theorem 4 also shows that $P_r(C_s > 0) = 1$ cannot be achieved.

V. Finite-Sized Cooperative HDR System

In this section, the secrecy performance of a finite-sized cooperative HDR system is derived as a baseline for comparison with the FDR system. A block diagram of a finite-sized cooperative HDR system can also be represented by Fig. 1, except that the source and relay transmit in two orthogonal time phases, so that the HDR node does not have an SI channel. At the tth block, the received signal at the relay and eavesdropper can be respectively expressed as

$$\begin{aligned} y_r(t) &= \sqrt{P_s\mathcal{L}_{1,k^*}}h_{1,k^*}\mathbb{I}_{k^*}x_s(t) + z_r(t) \text{ and} \\ y_e(t) &= \sqrt{P_s\mathcal{L}_{3,k^*}}h_{3,k^*}\mathbb{I}_{k^*}x_s(t) + z_e(t), \end{aligned} \tag{32}$$

where k^* is given by (1). At the $(t+1)$th block, the received signal at the destination and eavesdropper can be respectively expressed as

$$\begin{aligned} y_d(t+1) &= \sqrt{P_r\mathcal{L}_2}h_2x_s(t) + z_d(t+1) \text{ and} \\ y_e(t+1) &= \sqrt{P_r\mathcal{L}_4}h_4x_s(t) + z_e(t+1). \end{aligned} \tag{33}$$

The end-to-end SNR of the main relaying channel is given by $\gamma_{\rm HDR} = \min(\gamma_r, \gamma_d)$, where

$$\gamma_r \triangleq \frac{\mathbb{I}_{k^*}P_s\mathcal{L}_{1,k^*}|h_{1,k^*}|^2}{\sigma^2} \tag{34}$$

and γ_d is given by (8). The achievable maximum rate of the main relaying channel can be expressed as

$$C_{\rm HDR} = \frac{1}{2}\log_2(1+\gamma_{\rm HDR}), \tag{35}$$

where the pre-factor $\frac{1}{2}$ is resulted from HDR transmission. On the other hand, the eavesdropper receives the data $x_s(t)$ twice, from the selected transmitter at the tth block and the relay at the $(t+1)$th block, respectively. By assuming the eavesdropper can intelligently combine the received signal during two blocks [40], the achievable maximum rate of the eavesdropping channel can be expressed as

$$\begin{aligned} C_e^{\rm HDR} &= \frac{1}{2}\log_2\left(1 + \frac{P_s\mathcal{L}_{3,k^*}|h_{3,k^*}|^2\mathbb{I}_{k^*}}{\sigma^2} + \frac{P_r\mathcal{L}_4|h_4|^2}{\sigma^2}\right) \\ &= \frac{1}{2}\log_2(1+\gamma_e), \end{aligned} \tag{36}$$

where γ_e is given by (10). Substituting (35) and (36) into the secrecy capacity $C_s = [C_{\rm HDR} - C_e^{\rm HDR}]^+$, it can be shown

$$C_s = \frac{1}{2}\left[\log_2(1+\gamma_{\rm HDR}) - \log_2(1+\gamma_e)\right]^+. \tag{37}$$

Proposition 3. *The CDF of the SNR γ_r of the finite-sized cooperative HDR system is given by*

$$F_{\gamma_r}(x) = 1 + \sum_{k=1}^{K}\Upsilon(-1)^k\prod_{q=1}^{k}\left(\frac{s_{\ell_q}}{n_q!(\hat{\theta}_{1,\ell_q})^{n_q}}\right)e^{-\hat{\alpha}x}x^{\beta}, \tag{38}$$

where $\hat{\theta}_{1,k} \triangleq \frac{P_s\mathcal{L}_{1,k}\theta_{1,k}}{\sigma^2}$, $\hat{\alpha} \triangleq \sum_{q=1}^{k}\hat{\theta}_{1,\ell_q}^{-1}$, $\beta \triangleq \sum_{q=1}^{k}n_q$, *and*

$$\Upsilon \triangleq \sum_{\ell_1=1}^{K-k+1}\sum_{\ell_2=\ell_1+1}^{K-k+2}\cdots\sum_{\ell_k=\ell_{k-1}+1}^{K}\sum_{n_1=0}^{m_{1,\ell_1}-1}\sum_{n_2=0}^{m_{1,\ell_2}-1}\cdots\sum_{n_k=0}^{m_{1,\ell_k}-1}. \tag{39}$$

Proof: (38) can be derived by following the similar procedures as those in Appendix A. ■

By comparing (11) and (38), it can be shown that the CDF of γ_r of the HDR system has the same form as that of the FDR system, except $\hat{\theta}_{1,k}$ in the place of $\tilde{\theta}_{1,k}$ (note that $\hat{\alpha}$ is determined by $\hat{\theta}_{1,k}$). Since γ_d of the HDR system has the same form as that of the FDR system, the CDF of $\gamma_{\rm HDR}$ can be similarly derived as

$$\begin{aligned} F_{\gamma_{\rm HDR}}(x) &= 1 - \sum_{k=1}^{K}\Upsilon(-1)^{k+1}\prod_{q=1}^{k}\left(\frac{s_{\ell_q}}{n_q!(\hat{\theta}_{1,\ell_q})^{n_q}}\right) \\ &\qquad \sum_{n=0}^{m_2-1}\frac{1}{n!(\tilde{\theta}_2)^n}e^{-x(\hat{\alpha}+1/\tilde{\theta}_2)}x^{\beta+n}. \end{aligned} \tag{40}$$

The secrecy outage probability of the finite-sized cooperative HDR system can be expressed as

$$\begin{aligned} P_{\rm out} &= \Pr(C_s < R_s) \\ &= \int_0^{\infty}F_{\gamma_{\rm HDR}}(J_{\rm HDR}(1+x)-1)f_{\gamma_e}(x)\mathrm{d}x, \end{aligned} \tag{41}$$

where $J_{\rm HDR} \triangleq 2^{2R_s}$. Similarly to (24), the secrecy outage probability can be derived as (42) at the next page. In (42), we defined $\hat{\alpha} \triangleq \sum_{q=1}^{k}\hat{\theta}_{1,\ell_q}^{-1}$. Compared to the secrecy outage probability of the FDR system, $P_{\rm out}$ of (42) has the same form as that of (24) except the replacement of $\{\tilde{\theta}_{1,k}, J_{\rm FDR}\}$ with $\{\hat{\theta}_{1,k}, J_{\rm HDR}\}$. Since $\frac{\hat{\theta}_{1,k}}{\tilde{\theta}_{1,k}} = \gamma_{\rm RSI}$, (24) and (42) show that $\{\gamma_{\rm RSI}, J_{\rm FDR}, J_{\rm HDR}\}$ are the key parameters resulting in the different secrecy outage performances between the FDR and HDR systems. Since RSI can hardly be eliminated to the noise floor, we have $\tilde{\theta}_{1,k} < \hat{\theta}_{1,k}$ in practice. Thus, the effect of RSI on the secrecy outage probability cannot be ignored. Furthermore, we have $J_{\rm FDR} < J_{\rm HDR}$ due to FDR/HDR transmission, which also affects the corresponding secrecy outage probability.

For both the FDR and HDR systems, we know from (23) and (41) that $P_{\rm out} = 1$ for sufficiently large value of R_s. In contrast, when the secrecy rate R_s becomes extremely small ($R_s > 0$), we have the following proposition.

Proposition 4. *As R_s approaches 0, the secrecy outage probability of a finite-sized cooperative FDR/HDR system*

$$P_{\text{out}} = 1-\sum_{k=1}^{K}\Upsilon(-1)^{k+1}\prod_{q=1}^{k}\left(\frac{s_{\ell_q}}{n_q!(\hat{\theta}_{1,\ell_q})^{n_q}}\right)\sum_{n=0}^{m_2-1}\frac{1}{n!(\tilde{\theta}_2)^n}\sum_{i=0}^{\beta+n}\binom{\beta+n}{i}(J_{\text{HDR}}-1)^{\beta+n-i}J_{\text{HDR}}^{i}$$
$$e^{-(J_{\text{HDR}}-1)(\alpha+1/\tilde{\theta}_2)}\left[\frac{(1-s_{k^*})\Gamma(i+\breve{m}_2)}{\Gamma(\breve{m}_2)\breve{\theta}_2^{\breve{m}_2}}\left(J_{\text{HDR}}\hat{\alpha}+\frac{J_{\text{HDR}}}{\tilde{\theta}_2}+\frac{1}{\breve{\theta}_2}\right)^{-(i+\breve{m}_2)}\right.$$
$$\left.+s_{k^*}\sum_{\mu=1}^{2}\sum_{\nu=1}^{\breve{m}_\mu}\Xi_{\mu,\nu}\frac{\Gamma(i+\nu)}{\Gamma(\nu)\breve{\theta}_\mu^{\nu}}\left(J_{\text{HDR}}\hat{\alpha}+\frac{J_{\text{HDR}}}{\tilde{\theta}_2}+\frac{1}{\breve{\theta}_\mu}\right)^{-(i+\nu)}\right]. \quad (42)$$

---

with perfect backhaul but non-identical Nakagami-m fading is given by

$$P_{\text{out}} = 1-\sum_{k=1}^{K}\Upsilon(-1)^{k+1}\prod_{q=1}^{k}\left(\frac{1}{n_q!(\bar{\theta}_{1,\ell_q})^{n_q}}\right)\sum_{n=0}^{m_2-1}\sum_{\mu=1}^{2}\sum_{\nu=1}^{\breve{m}_\mu}\frac{\Xi_{\mu,\nu}}{n!(\tilde{\theta}_2)^n}\frac{\Gamma(\beta+n+\nu)}{\Gamma(\nu)\breve{\theta}_\mu^{\nu}}\left(\bar{\alpha}+\frac{1}{\tilde{\theta}_2}+\frac{1}{\breve{\theta}_\mu}\right)^{-(\beta+n+\nu)}, \quad (43)$$

where $\bar{\theta}_{1,\ell_q}=\tilde{\theta}_{1,\ell_q}$ for the FDR system, $\bar{\theta}_{1,\ell_q}=\hat{\theta}_{1,\ell_q}$ for the HDR system, and $\bar{\alpha}\triangleq\sum_{q=1}^{k}\bar{\theta}_{1,\ell_q}^{-1}$.

Proof: For the HDR system, J_{HDR} approaches 1 as R_s approaches 0. By substituting $s_k=1$, $J_{\text{HDR}}=1$, (16), and (40) into (41), we arrive at (43). Similarly, we prove the case for the FDR system. ■

Proposition 4 shows that the FDR/HDR transmission ($J_{\text{FDR}}/J_{\text{HDR}}$) has no effect on the secrecy outage probability when R_s becomes extremely small, while P_{out} is affected by Nakagami-m fading. For the FDR system, P_{out} is also affected by the RSI power level. If RSI is eliminated to the noise floor, i.e., $\gamma_{\text{RSI}}=0$ dB, we have $\tilde{\theta}_{1,k}=\hat{\theta}_{1,k}$. Thus, Proposition 4 indicates that the FDR and HDR systems achieve the same P_{out} with a small value of R_s given that RSI is well suppressed.

For the finite-sized cooperative HDR system, the probability of non-zero achievable secrecy rate can be expressed as

$$\Pr(C_s>0)=\int_0^\infty\bar{F}_{\gamma_{\text{HDR}}}(x)f_{\gamma_e}(x)\mathrm{d}x, \quad (44)$$

where $\bar{F}_{\gamma_{\text{HDR}}}(x)\triangleq 1-F_{\gamma_{\text{HDR}}}(x)$. Similarly to (26), the probability of non-zero achievable secrecy rate of the finite-sized cooperative HDR system can be evaluated as (45) at the next page. Note that (45) has the same form as that of (26) except the replacement of $\tilde{\theta}_{1,k}$ with $\hat{\theta}_{1,k}$. Thus, the FDR and HDR systems achieve the same probability of non-zero achievable secrecy rate only if RSI can be eliminated to the noise floor, i.e., $\tilde{\theta}_{1,k}=\hat{\theta}_{1,k}$. Since $\tilde{\theta}_{1,k}<\hat{\theta}_{1,k}$ in practice while RSI always deteriorates the $TX_k\to R$ link quality, it expects that the HDR system will achieve a higher $\Pr(C_s>0)$ than that of the FDR system.

Moreover, asymptotic secrecy outage probability and asymptotic probability of non-zero achievable secrecy rate of the finite-sized cooperative HDR system with perfect backhaul connections are given by (27) and (28), respectively, with substitutions of $J_{\text{FDR}}=J_{\text{HDR}}$ and $\tilde{\theta}_{1,k}=\hat{\theta}_{1,k}$ into the corresponding expressions, respectively. Consequently, the asymptotic secrecy performance limits achieved by the finite-sized cooperative HDR system are explicitly determined as

$$P_{\text{out}}^{as}=\prod_{k=1}^{K}(1-s_k)\quad\text{and} \quad (46)$$

$$\Pr^{as}(C_s^{\text{HDR}}>0)=1-\prod_{k=1}^{K}(1-s_k), \quad (47)$$

which have the same forms as those of the FDR system.

VI. Simulation Results

This section presents simulation results of the secrecy performance for the cooperative FDR system as well as the HDR counterpart. The link-level Monte Carlo simulations for the secrecy outage probability and probability of non-zero achievable secrecy rate are performed with the end-to-end SINR obtained from random channel realizations for all the links, while the analytical P_{out} and $\Pr(C_s>0)$ are evaluated for the FDR and HDR systems according to the expressions in Section IV and V, respectively. For notational convenience, analytical secrecy performance metrics with perfect backhauls are denoted by P_{out}^{∞} and $P_r^{\infty}(C_s>0)$, while the asymptotic secrecy performance limits with unreliable backhauls are denoted by $P_{\text{out}}^{as,K}$ and $P_r^{as,K}(C_s>0)$. In the simulations, we set $B=20$, $\tau=1$, $P_r=\chi_r P_s$, and consider the following scenarios to highlight the impact of key design parameters of the cooperative FDR system on the secrecy performance:

- S_1: $m_{1,k}=\{1,2\}$, $m_2=2$, $m_{3,k}=\{1,1\}$, $m_4=2$, $s_k=0.9$, $\chi_r=0.1$.
- S_2: $m_{1,k}=\{2,3\}$, $m_2=2$, $m_{3,k}=\{2,2\}$, $m_4=1$, $s_k=0.99$, $\chi_r=0.1$.
- S_3: $m_{1,k}=\{2,3,3\}$, $m_2=2$, $m_{3,k}=\{2,2,2\}$, $m_4=1$, $s_k=0.9$, $\chi_r=0.1$.
- S_4: $m_{1,k}=\{1,3,3\}$, $m_2=2$, $m_{3,k}=\{1,2,1\}$, $m_4=2$, $s_k=\{0.9,0.95,0.97\}$ or $s_k=\{0.8,0.85,0.87\}$, $\chi_r=0.1$.

A. Identical Backhaul Reliability

In Fig. 2, we verify the accuracy of the secrecy outage probability analysis for scenario S_1, where we set $P_s/\sigma^2=40$

$$\Pr(C_s > 0) = \sum_{k=1}^{K} \Upsilon(-1)^{k+1} \prod_{q=1}^{k} \left(\frac{s_{\ell_q}}{n_q! (\hat{\theta}_{1,\ell_q})^{n_q}} \right) \sum_{n=0}^{m_2-1} \frac{1}{n! (\tilde{\theta}_2)^n} \left[(1 - s_{k^*}) \frac{\Gamma(\beta + n + \breve{m}_2)}{\Gamma(\breve{m}_2) \breve{\theta}_2^{\breve{m}_2}} \left(\hat{\alpha} + \frac{1}{\tilde{\theta}_2} + \frac{1}{\breve{\theta}_2} \right)^{-(\beta+n+\breve{m}_2)} + s_{k^*} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \frac{\Gamma(\beta+n+\nu)}{\Gamma(\nu) \breve{\theta}_\mu^{\nu}} \left(\hat{\alpha} + \frac{1}{\tilde{\theta}_2} + \frac{1}{\breve{\theta}_\mu} \right)^{-(\beta+n+\nu)} \right]. \quad (45)$$

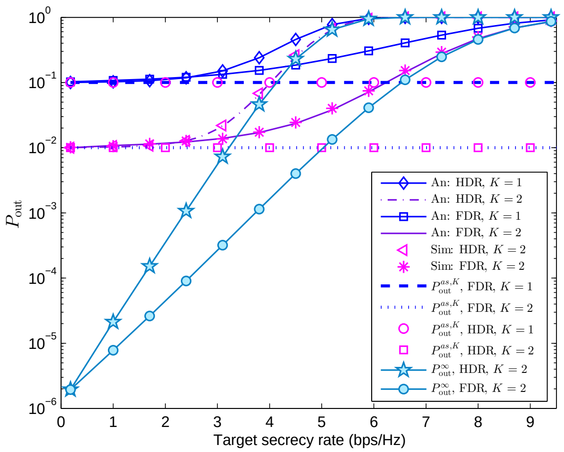

Fig. 2. Secrecy outage probability versus R_s at a fixed received SINR at the eavesdropper.

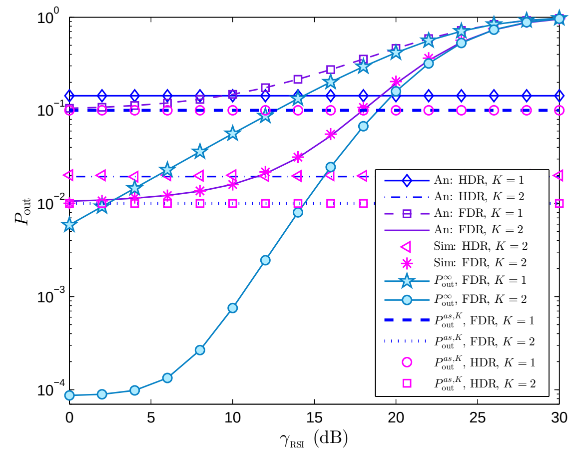

Fig. 3. Secrecy outage probability versus INR at a fixed received SINR at the eavesdropper.

dB and $\gamma_{\text{RSI}} = 8$ dB. As transmitter cooperation increases, Fig. 2 shows that both the secrecy outage probabilities of the FDR and HDR systems decrease. In the middle and large target secrecy rate region, the FDR system achieves a lower or equal secrecy outage probability compared to that of the HDR system. Independent of other parameters, it can be seen that $P_{\text{out}}^{as,K}$ is exclusively determined by backhaul reliability, $s_k = 0.9$. As $\tilde{\theta}_{1,k} \to \infty$ and $\breve{\theta}_2 \to \infty$, the secrecy outage probability limits can be evaluated as $P_{\text{out}}^{as,K} = 0.1$ and $P_{\text{out}}^{as,K} = 0.01$ for $K = 1$ and $K = 2$, respectively. When the target secrecy rate is small, Fig. 2 shows that P_{out} approaches the limits $P_{\text{out}}^{as,K}$ for both the FDR and HDR systems, as determined by (30) and (46). Moreover, as transmitter cooperation increases, a larger performance improvement can be achieved by the FDR system when it is not dominated by backhaul reliability. With increasing the target secrecy rate, P_{out} becomes large for both the FDR and HDR systems. As the target secrecy rate increases, P_{out} approaches P_{out}^{∞}. In contrast, when the target secrecy rate decreases to an extremely small value, Fig. 2 shows that the FDR and HDR achieves the same P_{out}^{∞} given that RSI is well suppressed ($\gamma_{\text{RSI}} = 8$ dB in this case), as indicated by Proposition 4.

In Fig. 3, we investigate the impact of RSI on the secrecy outage probability for scenario 1, where we set $P_s/\sigma^2 = 40$ dB and $R_s = 3$ bps/Hz. In the small γ_{RSI} region ($\gamma_{\text{RSI}} < 10$ dB), the FDR system achieves a lower secrecy outage probability than that of the HDR system. Therefore, less frequent secrecy outages happen only when RSI is relatively small. As γ_{RSI} decreases, the secrecy outage probability for the FDR system approaches $P_{\text{out}}^{as,K}$. With increasing γ_{RSI}, the secrecy outage probability of the FDR system also increases and approaches P_{out}^{∞} in the large γ_{RSI} region. As such, we can classify the operating region into two sub-regions based on the value of γ_{RSI}. In the small γ_{RSI} sub-region, we have $\tilde{\theta}_{1,k} \approx \hat{\theta}_{1,k}$, while (24) and (42) show that $\{J_{\text{FDR}}, J_{\text{HDR}}\}$ are the key parameters resulting in different P_{out}s for the FDR and HDR systems. Thus, the secrecy outage probability in the small γ_{RSI} sub-region is dominated by HDR/FDR transmission, i.e., $\{J_{\text{FDR}}, J_{\text{HDR}}\}$. In contrast, the secrecy outage probability in the large γ_{RSI} sub-region is dominated by RSI. Fig. 3 also verifies that the secrecy outage probability limit is exclusively determined by backhaul reliability given that $\tilde{\theta}_{1,k} \to \infty$ and $\breve{\theta}_2 \to \infty$. Note that $\tilde{\theta}_{1,k} \to \infty$ indicates that RSI needs be effectively eliminated to achieve $P_{\text{out}}^{as,K}$. Furthermore, Fig. 3 verifies that the FDR and HDR systems achieve the same $P_{\text{out}}^{as,K}$. Interestingly, we observe that there is a gap between $P_{\text{out}}^{as,K}$ and P_{out} for the HDR system, which indicates that the P_{out} of the HDR system cannot approach $P_{\text{out}}^{as,K}$ with the considered P_s/σ^2 ($P_s/\sigma^2 = 40$ dB in this case). In contrast, Fig. 3 also shows that the P_{out} of the HDR system approaches $P_{\text{out}}^{as,K}$ in the small γ_{RSI} region, which is beneficial from FDR transmission rather than HDR transmission. This will be further explained in the following Fig. 4. As γ_{RSI} decreases, Fig. 3 shows that P_{out}^{∞} for $K = 2$ reaches a floor, which is the smallest secrecy outage probability that can be achieved with the given P_s/σ^2. However, for $K = 1$, the smallest secrecy outage probability achieved by P_{out}^{∞} only occurs for $\gamma_{\text{RSI}} = 0$ dB. This phenomenon shows that transmitter cooperation can alleviate the burden of SI cancellation for the FDR system to achieve the allowable smallest secrecy outage probability.

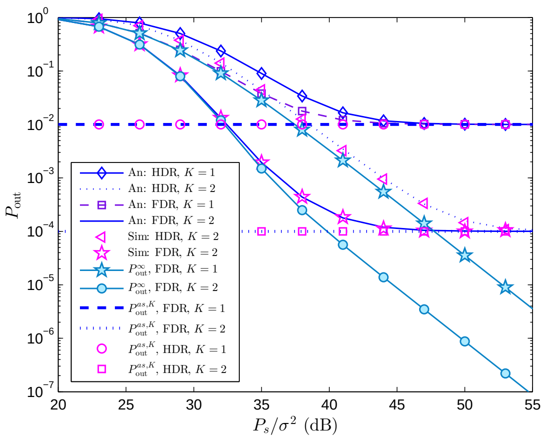

Fig. 4. Secrecy outage probability versus P_s/σ^2 at a fixed received SINR at the eavesdropper.

The secrecy outage probability versus P_s/σ^2 for scenario 2 is depicted in Fig. 4, where we set $\gamma_{\text{RSI}} = 8$ dB and $R_s = 3$ bps/Hz. The curves in Fig. 4 show that transmitter cooperation ($K = 1$ or 2) has no effect on the secrecy diversity gain, which verifies the correctness of Theorem 3. Furthermore, it can be verified that the outage diversity gain is $D = \min\left(\sum_{k=1}^{K} m_{1,k}, m_2\right) = 2$ by measuring the slope on a log-log plot. In the whole P_s/σ^2 region, it can be seen that the FDR system achieves a lower or equal secrecy outage probability compared to that of the HDR system. With $s_k = 0.99$ in scenario 2, Fig. 4 shows that $P_{\text{out}}^{as,K} = 0.01$ and $P_{\text{out}}^{as,K} = 0.0001$ for $K = 1$ and $K = 2$, respectively. With increasing P_s/σ^2, the secrecy outage probabilities for both the FDR and HDR systems decrease and finally approach $P_{\text{out}}^{as,K}$, while the FDR system approaches $P_{\text{out}}^{as,K}$ with a smaller P_s/σ^2 than that of the HDR system. Morover, in the low P_s/σ^2 region, the secrecy outage probabilities of the FDR and HDR systems with unreliable backhauls respectively approach the corresponding asymptotic limits with perfect backhauls.

In Fig. 5, we compare the secrecy outage probabilities between the FDR and HDR systems for scenario S_2 with $K = 2$. Under unreliable backhaul with $s_k = 0.99$, Fig. 5 shows that the secrecy outage probabilities of the FDR and HDR systems approach the same asymptotic limit $P_{\text{out}}^{as,K} = 10^{-4}$ with increasing P_s/σ^2. In contrast to the case of unreliable backhaul, the secrecy outage probability decreases with increasing P_s/σ^2 under perfect backhaul for both the FDR and HDR systems. When $\gamma_{\text{RSI}} = 5$ dB, the FDR system achieves a lower secrecy outage probability than that of the HDR system throughout the considered P_s/σ^2 region. When $\gamma_{\text{RSI}} = 15$ dB, the FDR system achieves a lower secrecy outage probability than that of the HDR system in the high P_s/σ^2 region. However, the FDR system with $\gamma_{\text{RSI}} = 15$ dB achieves a higher secrecy outage probability than that of the HDR system in the small and middle P_s/σ^2 regions. Moreover, for both

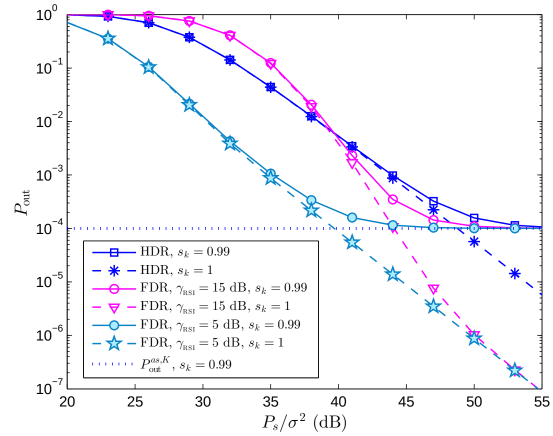

Fig. 5. Comparing P_{out} between FDR and HDR systems at a fixed received SINR at the eavesdropper.

the unreliable and perfect backhauls, the FDR (HDR) system achieves the same secrecy outage probability in the small and middle P_s/σ^2 regions.

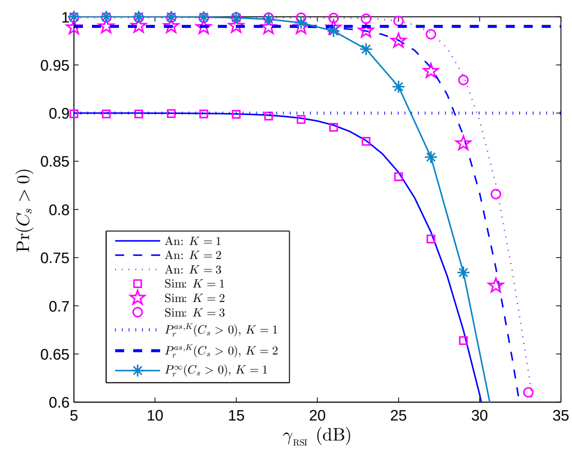

Fig. 6. $\Pr(C_s > 0)$ versus INR at a fixed received SINR at the eavesdropper.

Fig. 6 shows the impact of RSI on the probability of non-zero achievable secrecy rate for scenario S_3, where we set $P_s/\sigma^2 = 40$ dB. With increasing number of transmitters, the probability of non-zero achievable secrecy rate increases due to the increased received power at the relay. The probability of non-zero achievable secrecy rate decreases with increasing RSI. In the low γ_{RSI} region, the probability of non-zero achievable secrecy rate approaches the corresponding secrecy limit, which is mainly determined by backhaul reliability, i.e., $P_r^{as,K}(C_s) = 1 - (1 - s_k)^K$ with transmitter cooperation K and the backhaul reliability s_k. Moreover, Fig. 6 shows that with perfect backhaul reliability, the probability of non-zero achievable secrecy rate equals to 1 in the low γ_{RSI} region.

In Fig. 7, we investigate the probability of non-zero achievable secrecy rate versus P_s/σ^2 for scenario S_3, where we set $\gamma_{\text{RSI}} = 8$ dB. Interestingly, the probability of non-zero achievable secrecy rate of the HDR system is higher than that of the FDR system in the low and middle P_s/σ^2 regions, as expected by (45). Furthermore, both the FDR and HDR

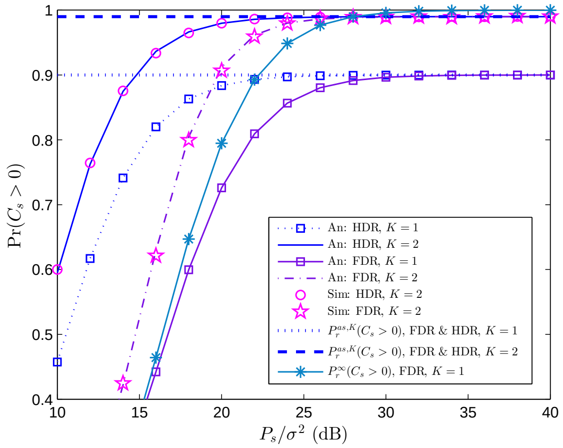

Fig. 7. $\Pr(C_s > 0)$ versus P_s/σ^2 at a fixed received SINR at the eavesdropper.

systems achieves a lower probability of non-zero achievable secrecy rate than $P_r^{as,K}$ in the low and middle P_s/σ^2 regions. With increasing P_s/σ^2, the probability of non-zero achievable secrecy rate approaches $P_r^{as,K}$, which is mainly determined by s_k and K. With perfect backhaul reliability, Fig. 7 also shows that $P_r^{\infty}(C_s > 0)$ approaches 1 in the high P_s/σ^2 region.

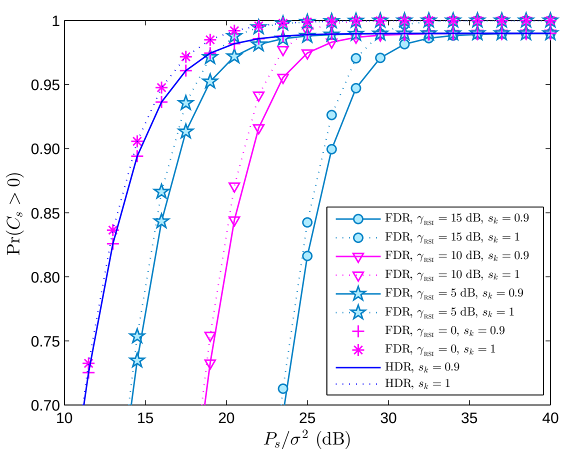

Fig. 8. Comparing $\Pr(C_s > 0)$ between FDR and HDR systems at a fixed received SINR at the eavesdropper.

In Fig. 8, we compare the probabilities of non-zero achievable secrecy rate between the FDR and HDR sytems for scenario S_2 with $K = 2$. Fig. 8 shows that the probability achieved with perfect backhaul ($s_k = 1$) is higher than that of the unreliable backhaul ($s_k = 0.9$), while the HDR system always achieves a higher $\Pr(C_s > 0)$ that of the FDR system suffering from RSI. With decreasing RSI from $\gamma_{\rm RSI} = 15$ dB to $\gamma_{\rm RSI} = 5$ dB, Fig. 8 shows that the $\Pr(C_s > 0)$ gap between the FDR and HDR systems also decreases. When RSI is completely cancelled ($\gamma_{\rm RSI} = 0$), the FDR system achieves the same $\Pr(C_s > 0)$ values as those of the HDR system. With increasing P_s/σ^2, $\Pr(C_s > 0)$ approaches the asymptotic limit, which is exclusively determined by the backhaul reliability, e.g., $P_r^{as,K}(C_s > 0) = 0.99$ for $s_k = 0.9$.

B. Non-Identical Backhaul Reliability

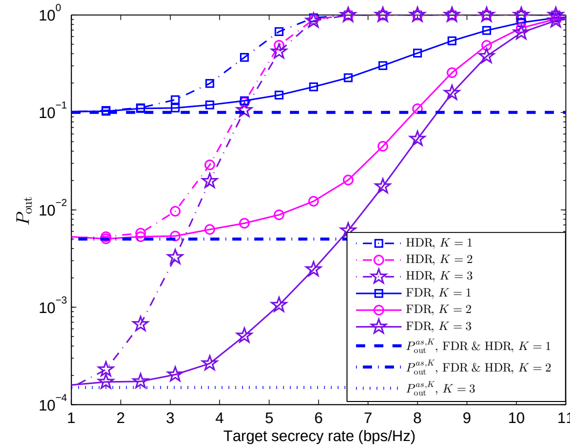

Fig. 9. Secrecy outage probability versus R_s at a fixed received SINR at the eavesdropper.

For scenario S_4 with $s_k = \{0.9, 0.95, 0.97\}$, the empirical secrecy outage probability and its asymptotic limit for non-identical backhaul reliability and non-identical Nakagami-m fading are depicted in Fig. 9, where we set $P_s/\sigma^2 = 40$ dB and $\gamma_{\rm RSI} = 5$ dB. From Theorem 4, the limit of secrecy outage probability is given by $P_{\rm out}^{as,K} = \prod_{k=1}^{K}(1 - s_k)$, which is evaluated as 1.0×10^{-1}, 5×10^{-3}, and 1.5×10^{-4} for $K = 1$, $K = 2$, and $K = 3$, respectively. Fig. 9 verifies that the empirical secrecy outage probabilities of both the FDR and HDR systems approach $P_{\rm out}^{as,K}$. Fig. 9 also shows that increasing transmitter cooperation results in decreasing empirical secrecy outage probability.

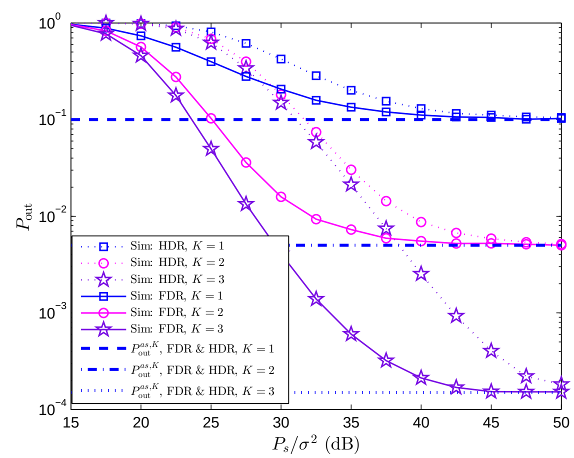

Fig. 10. Secrecy outage probability versus P_s/σ^2 at a fixed received SINR at the eavesdropper.

In Fig. 10, we investigate empirical secrecy outage probability versus P_s/σ^2 for the same scenario as that in Fig. 9. We set $\gamma_{\rm RSI} = 5$ dB and $R_s = 3$ bps/Hz in Fig. 10. The curves in Fig. 10 show that the empirical secrecy outage probability of the HDR system is higher than that of the FDR system in the considered P_s/σ^2 region. With increasing

P_s/σ^2, the empirical secrecy outage probability decreases and finally approaches $P_{\text{out}}^{as,K}$.

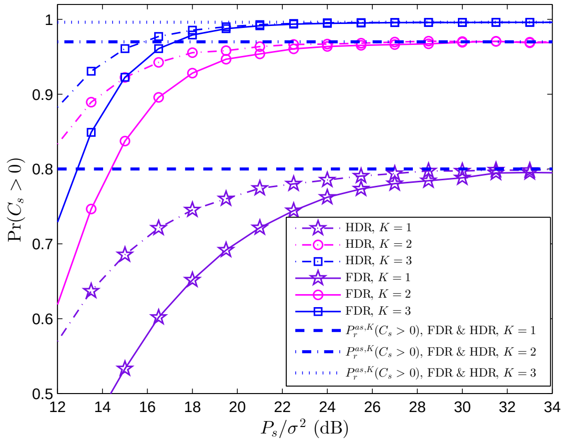

Fig. 11. $\Pr(C_s > 0)$ versus P_s/σ^2 at a fixed received SINR at the eavesdropper.

For scenario S_4 with $s_k = \{0.8, 0.85, 0.87\}$, Fig. 11 plots the probability of the non-zero achievable secrecy rate with non-identical backhaul and non-identical Nakagami-m fading, where we set $\gamma_{\text{RSI}} = 5$ dB. From Theorem 4, the asymptotic limit on the probability of the non-zero achievable secrecy rate is $\Pr^{as}(C_s^{\text{FDR}} > 0) = 1 - \prod_{k=1}^{K}(1 - s_k)$, which is exclusively determined by backhaul reliability. The correctness of this expression is readily verified by Fig. 11.

VII. Conclusion

This paper has investigated the impact of unreliable backhauls on the secrecy performance of a finite-sized cooperative FDR system. The secrecy outage probability and probability of non-zero achievable secrecy rate have been derived in closed-form for both the FDR and HDR systems. It has been shown that the secrecy performance of the FDR system is jointly affected by Nakagami-m fading, transmitter cooperation, backhaul reliability, and RSI. Due to full-duplex operation, the FDR system achieves a lower secrecy outage probability and a lower probability of non-zero achievable secrecy rate than those of the HDR system. Further, it has been shown that, with decreasing target secrecy rate, the secrecy outage probability of the FDR system converges to that of the HDR system, while the probability of non-zero achievable secrecy rate of the FDR system decreases with increasing RSI. In achieving the allowable smallest secrecy outage probability, transmitter cooperation can effectively alleviate the burden of SI cancellation for the FDR system. Moreover, both the FDR and HDR systems approach the same asymptotic secrecy performance limits, which are exclusively determined by unreliable backhauls.

Appendix A: Derivation of Proposition 1

Based on (7), the RV γ_r can be rewritten as

$$\gamma_r = \max_{k=1,\ldots,K} (\mathbb{I}_k X_{1,k}), \tag{A.1}$$

where $X_{1,k} \triangleq \frac{P_s \mathcal{L}_{1,k}|h_{1,k}|^2}{P_r|h_0|^2}$. Since that $X_{1,k} \sim \text{Ga}(m_{1,k}, \tilde{\theta}_{1,k})$, one particular RV $\mathbb{I}_k X_{1,k}$ in (A.1) has the following PDF

$$f_{\mathbb{I}_k X_{1,k}}(x) = (1 - s_k)\delta(x) + \frac{s_k x^{m_{1,k}-1} e^{-x/\tilde{\theta}_{1,k}}}{\Gamma(m_{1,k})(\tilde{\theta}_{1,k})^{m_{1,k}}} \tag{A.2}$$

and CDF

$$\begin{aligned} F_{\mathbb{I}_k X_{1,k}}(x) &= \int_0^x f_{\mathbb{I}_k X_{1,k}}(y)\mathrm{d}y \\ &= 1 - \frac{s_k \Gamma(m_{1,k}, x/\tilde{\theta}_{1,k})}{\Gamma(m_{1,k})}. \end{aligned} \tag{A.3}$$

After some mathematical manipulations, the CDF of γ_r can be expressed as

$$\begin{aligned} F_{\gamma_r}(x) &= \prod_{k=1}^{K} F_{\mathbb{I}_k X_{1,k}}(x) \\ &= \prod_{k=1}^{K} \left(1 - \frac{s_k \Gamma(m_{1,k}, x/\tilde{\theta}_{1,k})}{\Gamma(m_{1,k})}\right) \\ &= 1 + \sum_{k=1}^{K} \sum_{\ell_1=1}^{K-k+1} \sum_{\ell_2=\ell_1+1}^{K-k+2} \cdots \sum_{\ell_k=\ell_{k-1}+1}^{K} (-1)^k \\ &\quad \prod_{q=1}^{k} \left(\frac{s_{\ell_q} \Gamma(m_{1,\ell_q}, x/\tilde{\theta}_{1,\ell_q})}{\Gamma(m_{1,\ell_q})}\right). \end{aligned} \tag{A.4}$$

By assuming the shape factor $m_{1,k}$ a positive integer and substituting the series expansion of the upper gamma function [49, eq. 8.353/2] into (A.4), we have (A.5) at the next page. In (A.5), the summation over all combinations of links and shape factors is defined as

$$\Upsilon = \sum_{\ell_1=1}^{K-k+1} \sum_{\ell_2=\ell_1+1}^{K-k+2} \cdots \sum_{\ell_k=\ell_{k-1}+1}^{K} \sum_{n_1=0}^{m_{1,\ell_1}-1} \sum_{n_2=0}^{m_{1,\ell_2}-1} \cdots \sum_{n_k=0}^{m_{1,\ell_k}-1}. \tag{A.6}$$

Appendix B: Derivation of Theorem 1

The CDF of γ_r can be alternatively expressed as

$$\begin{aligned} F_{\gamma_r}(x) &= 1 - \sum_{k=1}^{K} \Upsilon (-1)^{k+1} \prod_{q=1}^{k} \left(\frac{s_{\ell_q}}{n_q!(\tilde{\theta}_{1,l_\ell})^{n_q}}\right) e^{-\alpha x} x^{\beta} \\ &= 1 - J_1, \end{aligned} \tag{B.1}$$

where

$$J_1 \triangleq \sum_{k=1}^{K} \Upsilon (-1)^{k+1} \prod_{q=1}^{k} \left(\frac{s_{\ell_q}}{n_q!(\tilde{\theta}_{1,\ell_q})^{n_q}}\right) e^{-\alpha x} x^{\beta}. \tag{B.2}$$

Since $\gamma_d \sim \text{Ga}(m_2, \tilde{\theta}_2)$, $1 - F_{\gamma_d}(x)$ is given by

$$1 - F_{\gamma_d}(x) = e^{-x/\tilde{\theta}_2} \sum_{n=0}^{m_2-1} \frac{1}{n!}\left(\frac{x}{\tilde{\theta}_2}\right)^n. \tag{B.3}$$

Substituting (B.1) and (B.3) into $F_{\gamma_{\text{FDR}}} = 1 - (1 - F_{\gamma_r}(x))(1 - F_{\gamma_d}(x))$, we have (13).

$$F_{\gamma_r}(x) = 1 + \sum_{k=1}^{K} \sum_{\ell_1=1}^{K-k+1} \sum_{\ell_2=\ell_1+1}^{K-k+2} \dots \sum_{\ell_k=\ell_{k-1}+1}^{K} (-1)^k \left(\prod_{q=1}^{k} s_{\ell_q} \right) e^{-\sum\limits_{q=1}^{k} \frac{x}{\tilde{\theta}_{1,\ell_q}}} \prod_{q=1}^{k} \left(\sum_{n=0}^{m_{1,\ell_q}-1} \frac{x^n}{n!(\tilde{\theta}_{1,\ell_q})^n} \right)$$
$$= 1 + \sum_{k=1}^{K} \Upsilon(-1)^k \prod_{q=1}^{k} \left(\frac{s_{\ell_q}}{n_q!(\tilde{\theta}_{1,\ell_q})^{n_q}} \right) e^{-\sum\limits_{q=1}^{k} \frac{x}{\tilde{\theta}_{1,\ell_q}}} x^{\sum\limits_{q=1}^{k} n_q}. \tag{A.5}$$

Appendix C: Derivation of Proposition 2

The SINR γ_e can be rewritten as $\gamma_e \triangleq Y_1 + Y_2$, where $Y_1 \triangleq P_s \mathcal{L}_{3,k^*} |h_{3,k^*}| \mathbb{I}_{k^*}/\sigma^2$ and $Y_2 \triangleq P_r \mathcal{L}_4 |h_4|^2/\sigma^2$. The RV Y_1 has the following PDF

$$f_{Y_1}(y) = (1 - s_{k^*})\delta(y) + \frac{s_{k^*} y^{\breve{m}_1 - 1} e^{-y/\breve{\theta}_1}}{\Gamma(\breve{m}_1)(\breve{\theta}_1)^{\breve{m}_1}} \tag{C.1}$$

and the CDF

$$F_{Y_1}(y) = 1 - \frac{s_{k^*} \Gamma(\breve{m}_1, y/\breve{\theta}_1)}{\Gamma(\breve{m}_1)}. \tag{C.2}$$

Since $Y_2 \sim \mathrm{Ga}(\breve{m}_2, \breve{\theta}_2)$, its PDF can be expressed as $f_{Y_2}(y) = f_{Z_{2,\breve{m}_2}}(y)$. Then, the PDF of γ_e can be evaluated as (C.3) at the next page. In (C.3), Θ can be interpreted as the PDF of the sum of two independent gamma random variables, which can be evaluated by applying the results of Theorem 1 and Corollary 1 of [50]. Then, we arrive at (16) and (17), respectively.

Appendix D: Derivation of Theorem 4

If the FDR node suppresses SI well, we can assume $\tilde{\theta}_{1,k} \to \infty$ in the high SNR region. As $\tilde{\theta}_{1,k} \to \infty$, the asymptotic CDF of γ_r with perfect backhaul ($s_k = 1$) can be expressed as

$$\begin{aligned} F_{\gamma_r}^{\tilde{\theta}_{1,k}\to\infty}(x) &= \prod_{k=1}^{K} \left(1 - \frac{\gamma(m_{1,k}, x/\tilde{\theta}_{1,k})}{\Gamma(m_{1,k})} \right) \\ &= \prod_{k=1}^{K} \left(1 - e^{-\frac{x}{\tilde{\theta}_{1,k}}} \sum_{\ell=0}^{m_{1,k}-1} \frac{1}{\ell!} \left(\frac{x}{\tilde{\theta}_{1,k}} \right)^{\ell} \right) \\ &\approx \prod_{k=1}^{K} \frac{1}{m_{1,k}!} \left(\frac{x}{\tilde{\theta}_{1,k}} \right)^{m_{1,k}}. \end{aligned} \tag{D.1}$$

The asymptotic CDF of γ_d as $\tilde{\theta}_2 \to \infty$ is given by $F_{\gamma_d}^{\tilde{\theta}_2\to\infty}(x) \approx \frac{1}{m_2!} \left(\frac{x}{\tilde{\theta}_2} \right)^{m_2}$. Then, the asymptotic expression for $F_{\gamma_{\mathrm{FDR}}}$ as $\tilde{\theta}_{1,k} \to \infty$ and $\tilde{\theta}_2 \to \infty$ can be expressed as (D.2) at the next page, where $\tilde{m}_{1,k} \triangleq \sum_{k=1}^{K} m_{1,k}$. With perfect backhaul ($s_k = 1$), γ_e becomes the sum of two independent gamma random variables. Applying (D.2) and (16) with $s_k = 1$ to (23), the asymptotic secrecy outage probability is derived as in (27). Similarly, by substituting (D.2) and (16) with $s_k = 1$ into (25) and solving the resulting integral, the asymptotic probability of non-zero secrecy rate is derived in (28).

Appendix E: Derivation of Theorem 5

For the asymptotic limits of the CDF of γ_{FDR}, we first derive the asymptotic CDFs of γ_r and γ_d, respectively. Assuming that SI has been well suppressed, the asymptotic CDF of γ_r in (11) as $\tilde{\theta}_{1,k} \to \infty$ becomes

$$\begin{aligned} F_{\gamma_r}(x) &= \prod_{k=1}^{K} \left(1 - \frac{s_k \Gamma(m_{1,k}, x/\tilde{\theta}_{1,k})}{\Gamma(m_{1,k})} \right) \\ &\approx \prod_{k=1}^{K} (1 - s_k) \end{aligned} \tag{E.1}$$

since $\Gamma(m_{1,k}, x/\tilde{\theta}_{1,k}) \to \Gamma(m_{1,k})$ as $\tilde{\theta}_{1,k} \to \infty$. Furthermore, the asymptotic CDF of γ_d as $\tilde{\theta}_2 \to \infty$ is given by

$$\begin{aligned} F_{\gamma_d}(x) &= 1 - e^{-x/\tilde{\theta}_2} \sum_{\ell=0}^{m_2-1} \frac{1}{\ell!} \left(\frac{x}{\tilde{\theta}_2} \right)^{\ell} \\ &\approx \frac{1}{m_2!} \left(\frac{x}{\tilde{\theta}_2} \right)^{m_2}. \end{aligned} \tag{E.2}$$

Therefore, the asymptotic limit of (13) is given by

$$\begin{aligned} F_{\gamma_{\mathrm{FDR}}}(x) &= F_{\gamma_r}(x) + F_{\gamma_d}(x) + F_{\gamma_r}(x) F_{\gamma_d}(x) \\ &= \prod_{k=1}^{K} (1 - s_k) \end{aligned} \tag{E.3}$$

since $F_{\gamma_d}(x)$ decays faster than $F_{\gamma_r}(x)$ as $\tilde{\theta}_{1,k}$, $\tilde{\theta}_2 \to \infty$.

For $f_{\gamma_e}(x) = f_{Y_\mu}(x)$, the asymptotic limit as $\breve{\theta}_\mu \to \infty$ is given by

$$\begin{aligned} f_{\gamma_e}(x) &= (1 - s_{k^*}) \frac{x^{\breve{m}_2 - 1}}{\Gamma(\breve{m}_2)(\breve{\theta}_2)^{\breve{m}_2}} + \\ & \quad s_{k^*} \sum_{\mu=1}^{2} \sum_{\nu=1}^{\breve{m}_\mu} \Xi_{\mu,\nu} \frac{x^{\nu-1}}{\Gamma(\nu)(\breve{\theta}_\mu)^{\nu}}. \end{aligned} \tag{E.4}$$

Applying (E.3) and (E.4) to the derivation of the secrecy outage probability results in

$$\begin{aligned} P_{\mathrm{out}}^{as} &= \int_0^\infty F_{\gamma_{\mathrm{FDR}}}(2^R(1+x) - 1) f_{\gamma_e}(x) \mathrm{d}x \\ &= \prod_{k=1}^{K} (1 - s_k) \end{aligned} \tag{E.5}$$

since $f_{\gamma_e}(x)$ decays faster than $F_{\gamma_{\mathrm{FDR}}}(x)$. Similarly, the asymptotic probability of non-zero secrecy rate is derived as

$$\begin{aligned} \Pr(C_s > 0) &= 1 - \int_0^\infty F_{\gamma_{\mathrm{FDR}}}(x) f_{\gamma_e}(x) \mathrm{d}x \\ &= 1 - \prod_{k=1}^{K} (1 - s_k). \end{aligned} \tag{E.6}$$

$$
\begin{aligned}
f_{\gamma_e}(x) &= \int_0^x f_{Y_1}(y) f_{Y_2}(x-y)\mathrm{d}y \\
&= \int_0^x (1-s_{k^*})\delta(y) f_{Y_2}(x-y)\mathrm{d}y + \int_0^x \frac{s_{k^*} y^{\breve{m}_1-1} e^{-y/\breve{\theta}_1}}{\Gamma(\breve{m}_1)(\breve{\theta}_1)^{\breve{m}_1}} f_{Y_2}(x-y)\mathrm{d}y \\
&= (1-s_{k^*}) f_{Y_2}(x) + \int_0^x \frac{s_{k^*} y^{\breve{m}_1-1} e^{-y/\breve{\theta}_1}}{\Gamma(\breve{m}_1)(\breve{\theta}_1)^{\breve{m}_1}} f_{Y_2}(x-y)\mathrm{d}y \\
&= (1-s_{k^*}) f_{Z_{2,\breve{m}_2}}(x) + s_{k^*} \underbrace{\int_0^x f_{Z_{1,\breve{m}_1}}(y) f_{Z_{2,\breve{m}_2}}(x-y)\mathrm{d}y}_{\Theta}.
\end{aligned} \tag{C.3}
$$

$$
F_{\gamma_{\mathrm{FDR}}}^{\tilde{\theta}_{1,k},\tilde{\theta}_2\to\infty} = \begin{cases} \prod_{k=1}^{K} \frac{1}{m_{1,k}!} \left(\frac{x}{\tilde{\theta}_{1,k}}\right)^{m_{1,k}} & m_2 > \tilde{m}_{1,k} \\ \frac{1}{m_2!} \left(\frac{x}{\tilde{\theta}_2}\right)^{m_2} & m_2 < \tilde{m}_{1,k} \\ \prod_{k=1}^{K} \frac{1}{m_{1,k}!} \left(\frac{x}{\tilde{\theta}_{1,k}}\right)^{m_{1,k}} + \frac{1}{m_2!} \left(\frac{x}{\tilde{\theta}_2}\right)^{m_2} & m_2 = \tilde{m}_{1,k}. \end{cases} \tag{D.2}
$$

REFERENCES

[1] J. Xu, J. Wang, Y. Zhu, Y. Yang, X. Zheng, S. Wang, L. Liu, K. Horneman, and Y. Teng, "Cooperative distributed optimization for the hyperdense small cell deployment," *IEEE Comm. Mag.*, vol. 52, no. 5, pp. 61–67, May 2014.

[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[3] J. G. Andrews, "Seven ways that HetNets are a cellular paradigm shift," *IEEE Commun. Mag.*, vol. 51, no. 3, pp. 136–144, Mar. 2013.

[4] Z. Mayer, J. Li, A. Papadogiannis, and T. Svensson, "On the impact of control channel reliability on coordinated multi-point transmission," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 28, pp. 1–16, 2014.

[5] S. Arad and J. Hoadley, *Systems and methods optimizing backhaul transport*. U.S. Patent 2014/0 160 939 A1, Jun. 12, 2014.

[6] S. Chia, M. Gasparroni, and P. Brick, "The next challenge for cellular networks: Backhaul," *IEEE Microw. Mag.*, vol. 10, no. 5, pp. 54–66, Aug. 2009.

[7] M. Coldrey, H. Koorapaty, J. E. Berg, Z. Ghebretensa, J. Hansryd, A. Derneryd, and S. Falahati, "Small-cell wireless backhauling: A non-line-of-sight approach for point-to-point microwave links," in *Proc. IEEE Veh. Technol. Conf.*, Québec City, Canada, 3-6 Sept. 2012, pp. 1–5.

[8] O. Tipmongkolsilp, S. Zaghloul, and A. Jukan, "The evolution of cellular backhaul technologies: Current issues and future trends," *IEEE Commun. Surv. Tuts.*, vol. 13, no. 1, pp. 97–113, 1st Quart. 2011.

[9] F. Pantisano, M. Bennis, W. Saad, M. Debbah, and M. Latva-Aho, "On the impact of heterogeneous backhauls on coordinated multipoint transmission in femtocell networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, 10-15 Jun. 2012, pp. 5064–5069.

[10] S. H. Park, O. Simeone, O. Sahin, and S. Shamai, "Multihop backhaul compression for the uplink of cloud radio access networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3185–3199, May 2016.

[11] D. Torrieri and M. C. Valenti, "The outage probability of a finite ad hoc network in nakagami fading," *IEEE Trans. Commun.*, vol. 60, no. 12, p. 2960C2970, Dec. 2012.

[12] S. Simeone, O. Somekh, E. Erkip, H. V. Poor, and S. Shamai, "Robust communication via decentralized processing with unreliable backhaul links," *IEEE Trans. Wireless Commun.*, vol. 57, no. 7, pp. 4187–4201, Jul. 2011.

[13] P. Ishwar, R. Puri, K. Ramchandran, and S. S. Pradhan, "On rate-constrained distributed estimation in unreliable sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 4, pp. 765–775, Apr. 2006.

[14] J. Du, M. Xiao, M. Skoglund, and M. Medard, "Wireless multicast relay networks with limited-rate source-conferencing," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1390–1401, Aug. 2013.

[15] G. Narlikar, G. Wilfong, and L. Zhang, "Designing multihop wireless backhaul networks with delay gurantees," *Wireless Netw.*, vol. 16, no. 1, pp. 237–254, Jan. 2010.

[16] H. Phan, F. Zheng, and M. Fitch, "Wireless backhaul networks with precoding complex field network coding," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 447–450, Mar. 2015.

[17] A. D. Coso and S. Simoens, "Distributed compression for MIMO coordinated networks with a backhaul constraint," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4698–4709, Sept. 2011.

[18] O. Simeone, O. Somekh, H. V. Poor, and S. Shamai, "Enhancing uplink throughput via local base station cooperation," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, 26-29 Oct. 2008, pp. 116–120.

[19] D. Bharadia, E. McMillin, and S. Katti, "Full duplex radios," in *Proc. ACM SIGCOMM*, Hong Kong, China, 12-16 Aug. 2013, pp. 1–12.

[20] T. Riihonen, S. Werner, and R. Wichman, "Optimized gain control for single-frequency relaying with loop interference," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2801–2806, Jun. 2009.

[21] I. Krikidis, H. Suraweera, P. Smith, and C. Yuen, "Full-duplex relay selection for amplify-and-forward cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4381–4393, Dec. 2012.

[22] H. Cui, M. Ma, L. Song, and B. Jiao, "Relay selection for two-way full duplex relay networks with amplify-and-forward protocol," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3768–3777, Jul. 2014.

[23] H. Suraweera, I. Krikidis, G. Zheng, C. Yuen, and P. Smith, "Low-complexity end-to-end performance optimization in MIMO full-duplex relay systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 913–927, Feb. 2014.

[24] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proc. 2013 ACM SIGCOMM*, Hong Kong, 12-16 Aug. 2013, pp. 375–386.

[25] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.

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

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

[28] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Taipe, Taiwan, Apr. 2009, pp. 1–5.

[29] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inform. Forensics and Security*, vol. 4, no. 4, pp. 242–256, Jun. 2009.

[30] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[31] X. Chen, C. Zhong, C. Yuen, and H. H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Comm. Mag.*, vol. 53, no. 12, pp. 40–46, Dec. 2015.

[32] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory 2007*, Nice, France, 24-29 Jun. 2007, pp. 2471–2475.

[33] A. Khisti and G. W. 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.

[34] H. Alves, R. D. Souza, and M. Debbah, "Enhanced physical layer security through transmit antenna selection," in *Proc. IEEE GLOBECOM Workshops*, Houston, TX, USA, 5-9 Dec. 2011, pp. 879–883.

[35] 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, Jun. 2012.

[36] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054–6067, Nov. 2014.

[37] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sept. 2015.

[38] J. Zhang, C. Yuen, C. K. Wen, S. Jin, K. K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. Inform. Forensics and Security*, vol. 11, no. 1, pp. 74–85, Jan. 2016.

[39] K. J. Kim, P. L. Yeoh, P. Orlik, and H. V. Poor, "Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections," *IEEE Trans. Signal Process.*, vol. 64, no. 17, pp. 4403–4416, Sept. 2016.

[40] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inform. Forensics and Security*, vol. 10, no. 3, pp. 574–583, Apr. 2015.

[41] S. Parsaeefard and T. L.-. Ngoc, "Improving wireless secrecy rate via full-duplex relay-assited protocols," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.

[42] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525–528, Apr. 2015.

[43] K. J. Kim, T. Khan, and P. Orlik, "Performance analysis of cooperative systems with unreliable backhauls and selection combining," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2448–2461, Mar. 2017.

[44] E. Ahmed and A. M. Eltawil, "All-digital self-interference cancellation technique for full-duplex systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3519–3532, Jul. 2015.

[45] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[46] M. G. Khafagy, A. Ismail, M. S. Alouini, and S. Aïssa, "Efficient cooperative protocols for full-duplex relaying over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3456–3470, Feb. 2015.

[47] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory 2006*, Seattle, WA, USA, 9-14 Jul. 2006, pp. 356–360.

[48] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory 2005*, Adelaide, SA, Australia, 4-9 Sept. 2005, pp. 2152–2155.

[49] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York: Academic Press, 2007.

[50] G. K. Karagiannidis, N. C. Sagias, and T. A. Tsiftsis, "Closed-form statistics for the sum of squared Nakagami-m variables and its applications," *IEEE Trans. Commun.*, vol. 54, no. 8, pp. 1353–1359, Aug. 2006.