Wireless Powered Large-Scale Multi-Antenna AF Relaying for Cooperative Jamming-Aided Secrecy

Hong Xing[†], Yansha Deng[†], Kai-Kit Wong[§] and Arumugam Nallanathan[†]

[†]Dept. of Informatics, King's College London. E-mails: $\{$hong.1.xing, yansha.deng, arumugam.nallanathan$\}$@kcl.ac.uk
[§]Dept. of Electronic and Electrical Engineering, University College London. E-mail: kai-kit.wong@ucl.ac.uk

***Abstract*—This paper studies the secrecy transmission with the aid of a large-scale multi-antenna amplify-and-forward (AF) relay wireless powered by the source. Specifically, the wireless energy harvesting (WEH)-enabled relay devices a hybrid receiver architecture, in which the received power at each individual antenna is split for energy harvesting (EH) and information receiving (IR) in the first transmission phase; the aggregate of the total harvested power is further split for cooperative jamming (CJ) to confound the eavesdroppers, and AF using maximum ratio combining (MRC) and maximum ratio transmitting (MRT), respectively, at the relay in the second transmission phase. Assuming that the eavesdroppers in the proximity are distributed as Poisson point process (PPP), no channel state information (CSI) but the density of which is known to the relay, the ergodic secrecy rate (ESR) is used to characterize the secrecy performance. The optimum portion of power allocated for CJ is also derived to significantly improve on the ESR especially in the case of high eavesdroppers' density.**

I. Introduction

Since privacy and security of data transmission has arisen as a major concern in ubiquitous wireless communications applications such as e-transactions, e-shoppings, and remote information collection and/or retrieving etc., *physical-layer security (PLS)* has been proposed as a promising solution to achieve wireless information-theoretic security [1] by leveraging intrinsic properties of wireless channels. Among various signal processing techniques in PLS, *cooperative jamming (CJ)*, which generates synthetic noise via cooperative nodes to obfuscate the eavesdroppers [2], has been substantially investigated (see [3] and references therein) to break through the "degraded eavesdropping channel" assumption.

One of the main obstacles that prohibit the CJ schemes from being employed is that the potential helpers are usually themselves energy starving. However, recent advances in wireless powered communication network (WPCN) (see [4] and references therein) have provided them with essential incentives to assist in secrecy communications. [5] considered to boost the secrecy information throughput via a wireless powered friendly jammer by judiciously designing power transfer/information transfer cycles. In addition, a self-sustaining *harvest-and-jam (HJ)* relaying protocol was proposed in [6], where the robust CJ covariance matrices against imperfect channel state information (CSI) were optimized subject to harvested energy constraints of HJ helpers.

The advantage of radio frequency (RF) wireless power transfer (WPT), notwithstanding its easy control, has been compromised by its low power transfer efficiency due to significant attenuation over distance as long as several meters. Large-scale MIMO [7] has thus been motivated as resolution for improving on WPT efficiency thanks to its enormous array gain [8]. The benefit of massive MIMO brought into PLS has also been studied in [9–12]. The secrecy performance of matched-filter (MF) precoding along with artificial noise (AN) generation was analyzed in [9] for multi-cell massive MIMO downlink transmission taking pilot contamination into account.

The promising feature of WPCN has been very recently embraced by massive MIMO for promoting wireless energy harvesting (WEH)-enabled secrecy cooperation. WEH-enabled amplify-and-forward (AF) relays have been early investigated in [13]. Later their receiver (Rx) structure was further optimized for purely *cooperative beamforming (CB)*, and joint CB and CJ in [14] and [15], respectively. Secret transmission assisted by a wireless powered massive MIMO relay through WPT from the source was considered in [16], where explicit expressions of secrecy outage capacity were derived under the assumption of imperfect legitimate CSI and no eavesdropper's CSI to show that the challenging "long transfer distance" issue has been well addressed.

The contribution of this paper are three-fold: the proposed Rx architecture for the wireless powered multi-antenna AF relay is, to the best knowledge of the authors, of the most general form incorporating per-antenna based power splitting (PS) and CJ synthesis; ergodic secrecy rate (ESR) is analyzed for the proposed CJ-aided AF relay beamforming under the practical assumption of no eavesdroppers' CSI but only their spatial density; optimum fraction of power allocation for CJ is obtained.

Notations—We use the uppercase boldface letters to denote matrices and lowercase boldface letters for vectors. The superscripts $(\cdot)^T$, $(\cdot)^\dagger$ and $(\cdot)^H$ denote the transpose, conjugate and conjugate transpose of either a vector or a matrix, respectively. $\|\cdot\|$ stands for the Euclidean norm of a vector, and the statistical expectation for a random variable is denoted by $\mathbb{E}[\cdot]$. $\mathbb{C}(\mathbb{R})^{x\times y}$ denotes the space of complex (real) matrices with dimensions specified by $x \times y$. Also, $\Gamma(\alpha) = \int_0^\infty \exp\{-t\}t^{\alpha-1}\mathrm{d}t$ is the gamma function [17, chap. 8.31]; $\Gamma(\alpha, x) = \int_x^\infty \exp\{-t\}t^{\alpha-1}\mathrm{d}t$ is the upper incomplete gamma function [17, chap. 8.35]. $d(\cdot,\cdot)$ represents the Euclidean distance between two points. Finally, $(x)^+$ denotes $\max(0, x)$.

II. System Model

In this paper, we consider secrecy transmission with the aid of a multi-antenna AF relay in a SWIPT system, where the transmitter (Tx) sends confidential message to the legitimate Rx far away from it exclusively via the multi-antenna AF relay[1] that is exposed to the illegal interception of a set of eavesdroppers as far as up to $R_{\max}$ away from it, denoted by $\mathcal{K} = \{1, 2, \ldots, K\}$, whose locations $\Phi_e = \{e_k | k \in \mathcal{K}\}$ are modelled as homogeneous Poisson point process (PPP) [19] (HPPP) with density λ_e. K is thus a Poisson random variable (RV) with mean $\mu = \lambda_e \pi (R_{\max}^2 - R_0^2))$, i.e., $\Pr(K = n) = \exp\{-\mu\}\mu^n/n!$. The eavesdroppers are also assumed to be distributed outside from a "security zone" centered at the source with a radius of R_0, since they are relatively easy to be detected within the immediate reach of the Tx otherwise [20]. Except for the large-scale antenna equipped AF relay, all the other nodes are equipped with single antenna each.

A two-hop half-duplex relaying protocol is considered to consist of two equal-time transmission slot, the duration of which is normalized to be one. The multi-antenna AF relay assumed to be solely powered by its wireless harvested energy from the Tx during the first transmission slot operates with the per-antenna-based power splitting (PS) that allows each antenna of the relay to harvest energy and to receive information from the same stream of received signal. It is shown in Fig. 1 that the ith antenna of the relay splits the received power of α_i for energy harvesting (EH) versus $1 - \alpha_i$ for information receiving (IR), $\forall i = \{1, \ldots, N\}$, upon receiving $\boldsymbol{y}_r$. The harvested energy is then accumulated to be further divided into two parts: one portion of ρ for generating a friendly jamming signal, and the other $1 - \rho$ for amplifying $\boldsymbol{y}'_r$.

The channel models consist of the large-scale path loss and the small-scale fast fading, i.e., $\boldsymbol{h}_{sr} = A_0^{\frac{1}{2}} \beta_{sr}^{-\frac{\alpha}{2}} \bar{\boldsymbol{h}}_{sr}$, $\boldsymbol{h}_{rd} = A_0^{\frac{1}{2}} \beta_{rd}^{-\frac{\alpha}{2}} \bar{\boldsymbol{h}}_{rd}$, and $\boldsymbol{h}_{re,k} = A_0^{\frac{1}{2}} \beta_{re,k}^{-\frac{\alpha}{2}} \bar{\boldsymbol{h}}_{re,k}$, $\forall k \in \mathcal{K}$, which denotes the complex channels from the source Tx to the relay, from the relay to the destined Rx, and from the relay to the kth eavesdropper, respectively. A_0 accounts for the free space path loss; $\beta_{jl} = \frac{d_{jl}}{d_0}$ denotes the distance from j to l with respect to (w.r.t.) a reference distance d_0, for $j \in \{\mathrm{s}, \mathrm{r}\}$ and $l \in \{\mathrm{r}, \mathrm{d}, \{\mathrm{e}, \mathrm{k}\}\}$; α is the path loss exponential factor; $\bar{\boldsymbol{h}}_{jl}$'s represent the small-scale fading that is considered to be independent Rayleigh fading, denoted by $\bar{\boldsymbol{h}}_{jl} \sim \mathcal{CN}(0, \boldsymbol{I})$. The CSI from and to the relay regarding the main channel is assumed to be known at the relay, while that regarding the eavesdroppers are kept unknown except for their spatial distribution density.

In the first transmission slot, the received signal at the front of the wireless powered AF relay is given by

$$\boldsymbol{y}_r = \sqrt{P_s A_0 \beta_{sr}^{-\alpha}} \bar{\boldsymbol{h}}_{sr} s + \boldsymbol{n}_a, \tag{1}$$

where s is a circularly symmetric complex Gaussian (CSCG) distributed RV, denoted by $s \sim \mathcal{CN}(0, 1)$. P_s denotes the source transmit power, and $\boldsymbol{n}_a$ is the additive white Gaussian noise (AWGN) with zero mean and covariance matrix $\sigma_{n_a}^2 \boldsymbol{I}$. In compliance with the antenna-wise PS receiver architecture shown in Fig. 1, the total aggregate of the wireless transferred power is identical to

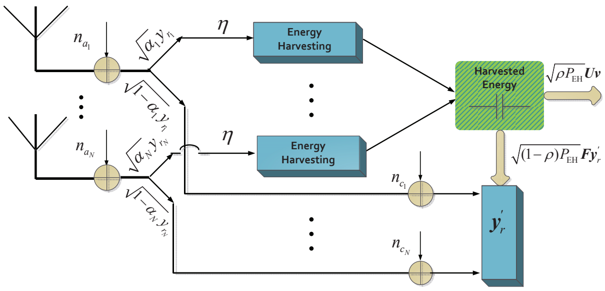
n_{a_1}
$\sqrt{\alpha_1} y_{r_1}$
η
Energy Harvesting
$\sqrt{1-\alpha_1} y_{r_1}$
n_{a_N}
$\sqrt{\alpha_N} y_{r_N}$
η
Energy Harvesting
$\sqrt{1-\alpha_N} y_{r_N}$
Harvested Energy
$\sqrt{\rho P_{\mathrm{EH}}} \boldsymbol{U}\boldsymbol{v}$
$\sqrt{(1-\rho) P_{\mathrm{EH}}} \boldsymbol{F}\boldsymbol{y}'_r$
n_{c_1}
n_{c_N}
$\boldsymbol{y}'_r$

Fig. 1. The PS protocol at the large-scale antenna equipped WEH-enabled AF relay.

$$\sum_{i=1}^{N} \eta(1-\rho) E[|\sqrt{\alpha_i} y_{r,i}|^2] = \eta P_s A_0 \beta_{sr}^{-\alpha} \|\boldsymbol{D}_\alpha \bar{\boldsymbol{h}}_{sr}\|^2, \tag{2}$$

denoted by P_{EH}, where $0 \le \eta < 1$ is the EH conversion efficiency, and $\boldsymbol{D}_\alpha = diag([\sqrt{\alpha_i}]_{i=1}^N)$. Simultaneously, the received signal that is fed into the input of the IR circuit of the relay (c.f. Fig. 1) is given by

$$\boldsymbol{y}'_r = \boldsymbol{D}_{\bar{\alpha}} (\sqrt{P_s A_0 \beta_{sr}^{-\alpha}} \bar{\boldsymbol{h}}_{sr} s + \boldsymbol{n}_a) + \boldsymbol{n}_c, \tag{3}$$

where $\boldsymbol{D}_{\bar{\alpha}} = diag([\sqrt{1-\alpha_i}]_{i=1}^N)$, and $\boldsymbol{n}_c \sim \mathcal{CN}(\boldsymbol{0}, \sigma_{n_c}^2 \boldsymbol{I})$ is the noise introduced by converting signal from RF band to base band.

The relay then further splits its harvested power with a fraction ρ: ρ for CJ vs $(1-\rho)$ for AF. The normalized amplified signal is expressed as $\bar{\boldsymbol{x}}_r = \boldsymbol{F}\boldsymbol{y}'_r$, where $\boldsymbol{F}$ is the beamforming matrix given by $\boldsymbol{F} =$

$$\frac{\bar{\boldsymbol{h}}_{rd}}{\|\bar{\boldsymbol{h}}_{rd}\|} \frac{(\boldsymbol{D}_{\bar{\alpha}}^{-1} \bar{\boldsymbol{h}}_{sr})^H}{\sqrt{\|\bar{\boldsymbol{h}}_{sr}\|^2 (P_s A_0 \beta_{sr}^{-\alpha} \|\bar{\boldsymbol{h}}_{sr}\|^2 + \sigma_{n_a}^2) + \sigma_{n_c}^2 \|\boldsymbol{D}_{\bar{\alpha}}^{-1} \bar{\boldsymbol{h}}_{sr}\|^2}}. \tag{4}$$

It is worthwhile noting that without (w/o) CSI of the eavesdroppers at the relay, we propose to use $\boldsymbol{F}$ in (4) since it achieves the optimal performance in conventional relaying system w/o secrecy concern by jointly implementing linear precoding, i.e., maximum ratio combining (MRC) and maximum ratio transmitting (MRT), at the Rx and the Tx of the relay, respectively. The CJ signal is expressed as $\bar{\boldsymbol{x}}_j = \boldsymbol{U}\boldsymbol{v}$, where $\boldsymbol{U} \in \mathbb{C}^{N \times (N-1)}$ is made orthogonal to $\bar{\boldsymbol{h}}_{rd}$ such that $\boldsymbol{U}\boldsymbol{U}^H = \boldsymbol{I} - \bar{\boldsymbol{h}}_{rd} \bar{\boldsymbol{h}}_{rd}^H / \|\boldsymbol{h}_{rd}\|^2$, and $\boldsymbol{v}$ is composed of $i.i.d.$ CSCG RV with zero mean and variance $1/N - 1$. As such, the signal to be forwarded is expressed as a whole by

$$\boldsymbol{x}_r = \sqrt{(1-\rho) P_{\mathrm{EH}}} \bar{\boldsymbol{x}}_r + \sqrt{\rho P_{\mathrm{EH}}} \bar{\boldsymbol{x}}_j. \tag{5}$$

In the second transmission slot, the signal received by the destination is thus expressed as

$$y_d = \sqrt{A_0 \beta_{rd}^{-\alpha}} \bar{\boldsymbol{h}}_{rd}^H \boldsymbol{x}_r + n_d, \tag{6}$$

[1] Direct links from the Tx to the Rx and/or eavesdroppers are assumed to be broken due to severe path loss caused by constructions [18].

where $n_d \sim \mathcal{CN}(0, \sigma_{n_d}^2)$ is the AWGN at the destination Rx. By substituting (5) into (6) with $\boldsymbol{F}$ replaced by (4), y_d can be recast as follows.

$$\begin{aligned} y_d = c_1 \sqrt{P_s A_0 \beta_{sr}^{-\alpha}} \|\bar{\boldsymbol{h}}_{sr}\|^2 s + c_1 \bar{\boldsymbol{h}}_{sr}^H \boldsymbol{n}_a \\ + c_1 \bar{\boldsymbol{h}}_{sr}^H \boldsymbol{D}_{\bar{\alpha}}^{-1} \boldsymbol{n}_c + n_d, \end{aligned} \tag{7}$$

where

$$c_1 = \sqrt{\frac{\eta(1-\rho) P_s A_0^2 \beta_{sr}^{-\alpha} \beta_{rd}^{-\alpha} \|\boldsymbol{D}_\alpha \bar{\boldsymbol{h}}_{sr}\|^2 \|\bar{\boldsymbol{h}}_{rd}\|^2}{\|\bar{\boldsymbol{h}}_{sr}\|^2 (P_s A_0 \beta_{sr}^{-\alpha} \|\bar{\boldsymbol{h}}_{sr}\|^2 + \sigma_{n_a}^2) + \sigma_{n_c}^2 \|\boldsymbol{D}_{\bar{\alpha}}^{-1} \bar{\boldsymbol{h}}_{sr}\|^2}}. \tag{8}$$

Similarly, it follows that

$$\begin{aligned} y_{e,k} = c_{2,k} \sqrt{P_s A_0 \beta_{sr}^{-\alpha}} \|\bar{\boldsymbol{h}}_{sr}\|^2 s + c_{2,k} \bar{\boldsymbol{h}}_{sr}^H \boldsymbol{n}_a \\ + c_{2,k} \bar{\boldsymbol{h}}_{sr}^H \boldsymbol{D}_{\bar{\alpha}}^{-1} \boldsymbol{n}_c + c_{3,k} \bar{\boldsymbol{h}}_{re,k}^H \boldsymbol{U} \boldsymbol{v} + n_{e,k}, \end{aligned} \tag{9}$$

where $n_{e,k}$'s are the AWGN at the kth eavesdropper, denoted by $n_{e,k} \sim \mathcal{CN}(0, \sigma_{n_e}^2)$, $c_{2,k} =$

$$\sqrt{\frac{\eta(1-\rho) P_s A_0^2 \beta_{sr}^{-\alpha} \beta_{re,k}^{-\alpha} \|\boldsymbol{D}_\alpha \bar{\boldsymbol{h}}_{sr}\|^2}{\|\bar{\boldsymbol{h}}_{sr}\|^2 (P_s A_0 \beta_{sr}^{-\alpha} \|\bar{\boldsymbol{h}}_{sr}\|^2 + \sigma_{n_a}^2) + \sigma_{n_c}^2 \|\boldsymbol{D}_{\bar{\alpha}}^{-1} \bar{\boldsymbol{h}}_{sr}\|^2}} \frac{\bar{\boldsymbol{h}}_{re,k}^H \bar{\boldsymbol{h}}_{r,d}}{\|\bar{\boldsymbol{h}}_{r,d}\|}, \tag{10}$$

and

$$c_{3,k} = \sqrt{\eta\rho(1-\rho) P_s A_0^2 \beta_{sr}^{-\alpha} \beta_{re,k}^{-\alpha} \|\boldsymbol{D}_\alpha \bar{\boldsymbol{h}}_{sr}\|^2}. \tag{11}$$

In accordance with (7) and (9), the corresponding signal-to-interference-plus-noise ratio (SINR) of the destination and the kth eavesdropper, $\forall k \in \mathcal{K}$, can be expressed, respectively, as (12) and (13) shown at the top of the next page.

III. Large-Scale Antenna Based Secrecy Performance

In this section, assuming that the number of antennas equipped at the WEH-enabled AF relay tends to be very large, the cumulative density functions (CDFs) of the destination and/or the eavesdroppers' SINRs are first characterized, based on which the ergodic secrecy rate (ESR) of the considered system is evaluated. Then the optimum power allocation between the wireless powered CJ and AF is derived to achieve the maximum ESR. Prior to analyzing the ergodic secrecy rate, the instantaneous SINR of the destination and the eavesdroppers are first approximated by the following two lemmas, respectively.

Lemma 3.1: The instantaneous SINR of the destination can be approximated by

$$\mathrm{SINR}_{r,d} \xrightarrow[N \to \infty]{\text{a.s.}} \frac{N_1}{D_1}, \tag{14}$$

where

$$N_1 = \eta(1-\rho) P_s A_0^2 \beta_{sr}^{-\alpha} \beta_{rd}^{-\alpha} c_N \sum_{i=1}^{N} \alpha_i, \tag{15}$$

where $c_N = N^2 + N$, and

$$\begin{aligned} D_1 = \eta(1-\rho) A_0 \beta_{rd}^{-\alpha} \sum_{i=1}^{N} \alpha_i \left(\sigma_{n_a}^2 N + \sigma_{n_c}^2 \sum_{i=1}^{N} \frac{1}{1-\alpha_i} \right) \\ + \sigma_{n_d}^2 c_5, \end{aligned} \tag{16}$$

where $c_5 = \frac{c_N}{N} + \frac{\sigma_{n_c}^2 \sum_{i=1}^{N} \frac{1}{1-\alpha_i}}{P_s A_0 \beta_{sr}^{-\alpha} N} + \frac{\sigma_{n_a}^2}{P_s A_0 \beta_{sr}^{-\alpha}}$, when the number of relay antennas N tends to be very large.

Proof: In accordance with the law of large numbers [21, Th. 8.1], for $\bar{\boldsymbol{h}}_{sr} \sim \mathcal{CN}(0, \boldsymbol{I})$, we have $\|\bar{\boldsymbol{h}}_{sr}\|^4 \xrightarrow[N \to \infty]{\text{a.s.}} c_N$, $\|\bar{\boldsymbol{h}}_{sr}\|^2/N \xrightarrow[N \to \infty]{\text{a.s.}} 1$, $\left\|\boldsymbol{D}_{\bar{\alpha}}^{-1} \bar{\boldsymbol{h}}_{sr}\right\|^2 \xrightarrow[N \to \infty]{\text{a.s.}} \sum_{i=1}^{N} \frac{1}{1-\alpha_i}$, and $\left\|\boldsymbol{D}_\alpha \bar{\boldsymbol{h}}_{sr}\right\|^2 \xrightarrow[N \to \infty]{\text{a.s.}} \sum_{i=1}^{N} \alpha_i$, which can be plugged into (12), and Lemma 3.1 thus follows. ■

Lemma 3.2: The instantaneous SINR of the kth eavesdropper, $k \in \mathcal{K}$, can be approximated by

$$\mathrm{SINR}_{re,k} \xrightarrow[N \to \infty]{\text{a.s.}} \frac{N_2}{D_{2,k}}, \tag{17}$$

where

$$N_2 = \eta(1-\rho) P_s A_0^2 \beta_{sr}^{-\alpha} \beta_{re,k}{}^{-\alpha} c_N |Z_k|^2 \sum_{i=1}^{N} \alpha_i, \tag{18}$$

and

$$\begin{aligned} D_{2,k} = \eta(1-\rho) A_0 \beta_{re,k}{}^{-\alpha} |Z_k|^2 \sum_{i=1}^{N} \alpha_i \Big(\sigma_{n_a}^2 N \\ + \sigma_{n_c}^2 \sum_{i=1}^{N} 1/(1-\alpha_i) \Big) + c_5 N + \Big(\sigma_{n_e}^2 \\ + \eta\rho(1-\rho) P_s A_0^2 \beta_{sr}^{-\alpha} \beta_{re,k}^{-\alpha} \sum_{i=1}^{N} \alpha_i \Big), \end{aligned} \tag{19}$$

where $Z_k = \bar{\boldsymbol{h}}_{re,k}^H \frac{\bar{\boldsymbol{h}}_{r,d}}{\|\bar{\boldsymbol{h}}_{r,d}\|}$, $\forall k \in \mathcal{K}$, when the number of relay antennas N tends to be very large.

Proof: In addition to the known results from the proof for Lemma 3.1, we have $\|\boldsymbol{U}^H \bar{\boldsymbol{h}}_{re,k}\|^2/N \xrightarrow[N \to \infty]{\text{a.s.}} 1$, since $\boldsymbol{U}^H \bar{\boldsymbol{h}}_{re,k} \sim \mathcal{CN}(0, \boldsymbol{I})$ as a result of $\boldsymbol{U}^H \boldsymbol{U} = \boldsymbol{I}$. ■

Note that conditioned on HPPP, it is shown in (14) that the instantaneous SINR of the destination remains deterministic, while that of the kth eavesdropper turns out to be stochastic due toZ_k's that are *i.i.d.* RVs denoted by $Z_k \sim \mathcal{CN}(0, 1)$ [9, *Lemma 1*]. Hence, only the CDFs of the eavesdroppers remain relevant in terms of the ergodic secrecy rate. Besides, it is seen shortly that the achievable secrecy rate of a wiretap channel is only determined by the most detrimental eavesdropper, i.e., the one with the maximum eavesdropping channel capacity. Hence, the CDF of the maximum eavesdropping SINR is provided by the following proposition.

Proposition 3.1: The CDF of the maximum instantaneous $\mathrm{SINR}_{re,k}$ is derived as $F_\Upsilon(\upsilon) =$

$$\begin{cases} \exp\Bigg\{ -\frac{\lambda_e}{\alpha} \exp\left\{-\Delta |c_4|^2 \upsilon\right\} (\Delta\upsilon)^{-2/\alpha} \Big[\pi \Gamma\left(\frac{2}{\alpha}\right) \\ + \int_{\pi/2}^{3\pi/2} \Gamma\left(\frac{2}{\alpha}, \Delta\upsilon \left(-2R_0 \cos\theta\right)^{\alpha}\right) \mathrm{d}\theta \Big] \Bigg\} & \text{if } \upsilon < \upsilon_{\mathrm{th}}, \\ 1 & \text{otherwise.} \end{cases} \tag{20}$$

$$\mathrm{SINR}_{r,d} = \frac{|c_1|^2 P_s A_0 \beta_{sr}^{-\alpha} \|\bar{\boldsymbol{h}}_{sr}\|^4}{\sigma_{n_a}^2 |c_1|^2 \|\bar{\boldsymbol{h}}_{sr}\|^2 + \sigma_{n_c}^2 |c_1|^2 \|\boldsymbol{D}_{\bar{\alpha}}^{-1} \bar{\boldsymbol{h}}_{sr}\|^2 + \sigma_{n_d}^2} \tag{12}$$

$$\mathrm{SINR}_{re,k} = \frac{|c_{2,k}|^2 P_s A_0 \beta_{sr}^{-\alpha} \|\bar{\boldsymbol{h}}_{sr}\|^4}{\sigma_{n_a}^2 |c_{2,k}|^2 \|\bar{\boldsymbol{h}}_{sr}\|^2 + \sigma_{n_c}^2 |c_{2,k}|^2 \|\boldsymbol{D}_{\bar{\alpha}}^{-1} \bar{\boldsymbol{h}}_{sr}\|^2 + \sigma_{n_e}^2 + \sigma_v^2 |c_{3,k}|^2 \|\boldsymbol{U}^H \bar{\boldsymbol{h}}_{re,k}\|^2} \tag{13}$$

where

$$\Delta = \sigma_{n_e}^2 \Big(c_N + \frac{\sigma_{n_c}^2 \sum_{i=1}^N \frac{1}{1-\alpha_i} + \sigma_{n_a}^2 N}{P_s A_0 \beta_{sr}^{-\alpha}} \Big) / \Big(\eta (1-\rho) A_0 \sum_{i=1}^N \alpha_i \Big(P_s A_0 \beta_{sr}^{-\alpha} c_N - \upsilon \big(\sigma_{n_a}^2 N + \sigma_{n_c}^2 \sum_{i=1}^N \frac{1}{1-\alpha_i} \big) \Big) \Big), \tag{21}$$

and $\upsilon_{\mathrm{th}} = P_s A_0 \beta_{sr}^{-\alpha} c_N / (\sigma_{n_a}^2 N + \sigma_{n_c}^2 \sum_{i=1}^N 1/(1-\alpha_i))$.

Proof: First, the CDF of the maximum instantaneous SINR among the eavesdroppers conditioned on HPPP is defined as

$$\begin{aligned} F_\Upsilon(\upsilon) &= \mathbb{E}_{\Phi_e} \left[\Pr \left\{ \max_{e_k \in \Phi_e} \{\mathrm{SINR}_{re,k}\} \leq \upsilon \middle| \Phi_e \right\} \right] \\ &= \mathbb{E}_{\Phi_e} \left[\prod_{e_k \in \Phi_e} \Pr \left\{ |Z_k|^2 \leq \Delta\upsilon \left(|\beta_{re,k}|^\alpha + |c_{4,k}|^2 \right) \middle| \Phi_e \right\} \right] \\ &= \mathbb{E}_{\Phi_e} \left[\prod_{e_k \in \Phi_e} \left[1 - \exp\left\{ -\Delta\upsilon \left(|\beta_{re,k}|^\alpha + |c_{4,k}|^2 \right) \right\} \right] \right], \end{aligned} \tag{22}$$

where $c_4 = \sqrt{\eta\rho(1-\rho) P_s A_0^2 \beta_{sr}^{-\alpha} \sum_{i=1}^N \alpha_i / \sigma_{n_e}^2}$.

Next, by using the Generating functional of HPPP , we solve (22) as

$$\begin{aligned} F_\Upsilon(\upsilon) &= \exp\left\{ -\lambda_e \int_{\mathcal{S}} \exp\left\{ -\Delta\upsilon \left(|\beta_{re,k}|^\alpha + |c_4|^2 \right) \right\} \mathrm{d}A \right\} \\ &\overset{(a)}{=} \exp\left\{ -\lambda_e \int_{-\pi/2}^{\pi/2} \int_{(-2R_0\cos(\theta))^+}^{\infty} \exp\left\{ -\Delta\upsilon \left(r^\alpha + |c_4|^2 \right) \right\} r \mathrm{d}r \mathrm{d}\theta \right\} = \exp\Bigg\{ -\frac{\lambda_e}{\alpha} \exp\left\{ -\Delta |c_4|^2 \upsilon \right\} (\Delta\upsilon)^{-2/\alpha} \\ &\quad \left[\pi \Gamma\left(\frac{2}{\alpha} \right) + \int_{\pi/2}^{3\pi/2} \Gamma\left(\frac{2}{\alpha}, \Delta\upsilon \left(-2R_0 \cos\theta \right)^\alpha \right) \mathrm{d}\theta \right] \Bigg\}, \end{aligned} \tag{23}$$

where $\mathcal{S} = \{e_k \in \Phi_e | d(\mathrm{Tx}, e_k) \geq R_0\}$ as accounted earlier in Section II, which is equivalent to $\sqrt{r^2 + R_0^2 - 2rR_0\cos(\theta)} \geq R_0$ in polar coordinate originated at the relay, and thus leads to (a). ■

A. Ergodic Secrecy Rate

The achievable instantaneous secrecy rate [2] conditioned on Φ_e is given by $r_{\mathrm{sec}}^{(\mathrm{inst})} =$

$$\frac{1}{2} \Bigg(\log_2 \left(1 + \mathrm{SINR}_{rd} \right) - \log_2 \left(1 + \max_{e_k \in \Phi_k} \mathrm{SINR}_{re,k} \right) \Bigg)^+, \tag{24}$$

where $1/2$ accounts for the two transmission slot. Plugging into (24) (14) and (17), the approximate expression for $r_{\mathrm{sec}}^{(\mathrm{inst})}$ when the number of relay antennas N tends to be very large is thus obtained. Considering the no-delay-limited secrecy information transmission to the destination, ESR is a relevant metric that is given by [22] $r_{\mathrm{sec}} =$

$$\frac{1}{2} \Bigg(\log_2 \left(1 + \frac{N_1}{D_1} \right) - \mathbb{E}_{\Phi_e} \left[\log_2 \left(1 + \max_{e_k \in \Phi_e} \frac{N_2}{D_{2,k}} \right) \right] \Bigg)^+. \tag{25}$$

To calculate (25), we need the following lemma.

Lemma 3.3: Given a RV Υ with a continuous CDF $F_\Upsilon(\upsilon)$ defined on $[0, \infty)$, it holds true that

$$\mathbb{E}_\Upsilon \left[\log_2(1 + \Upsilon) \right] = \frac{1}{\ln 2} \int_0^\infty \frac{1}{1+\upsilon} \left(1 - F_\Upsilon(\upsilon) \right) \mathrm{d}\upsilon. \tag{26}$$

Substitute the CDF of the most detrimental $\mathrm{SINR}_{re,k}$ derived in (20) into (26), the ESR defined by (25) can be derived as (27) at the top of the next page.

B. Optimal Power Allocations for CJ

The proper ρ portion of the harvested power needs to be judiciously allocated, since the amount of CJ power is supposed to be, on one hand, sufficient for combating as many as an expectation of $\lambda_e \pi (R_{\max}^2 - R_0^2)$ eavesdroppers, and on the other hand, not too much to degrade the secrecy information transmission. The ρ that achieves the optimal trade-off between effective CJ and information AF is obtained by solving the following problem.

$$\underset{0 \leq \rho \leq 1}{\mathtt{Maximize}} \quad r_{\mathrm{sec}}(\rho) \text{ (c.f. (27))}. \tag{28}$$

It is easily seen from (27) that $r_{\mathrm{sec}}(\rho)$ is continuous w.r.t. ρ over $[0, 1]$, and thus according to Weierstrass theorem, $r_{\mathrm{sec}}(\rho)$ can admit its maximum when ρ takes its optimum value, denoted by ρ^*. To obtain ρ^*, we need the following proposition.

Proposition 3.2:

$$\rho^* = \arg\max\{r_{\mathrm{sec}}(0), r_{\mathrm{sec}}(\chi)\}, \tag{29}$$

where χ is a set defined as $\chi = \{\rho \in [0, 1] \mid f(\rho) = 0\}$, and $r_{\mathrm{sec}}(\chi)$ denotes the finite list of r_{sec}'s corresponding to each element of χ. $f(\rho)$ is given by (30), in which A, B, and C have already been given in (27); $E = \frac{-2}{\alpha^2} (\Delta\upsilon)^{-2/\alpha} / (1 - \rho)$; D and F are given by (31) and (32), respectively.

Proof: To derive ρ^*, we take $\frac{\partial r_{\mathrm{sec}}(\rho)}{\partial \rho}$, denoted by $f(\rho)$, and solve $f(\rho) = 0$, which yields a transcendental equation that is hard to obtain its closed-form solutions. However, since (30) is continuous w.r.t. ρ over $[0, 1)$, this equation can be solved by numerical means. As a special case, if $\chi = \emptyset$, which implies $f(\rho) < 0$ over $[0, 1)$, ρ^* is 0. This completes the proof. ■

$$r_{\mathrm{sec}} = \frac{1}{2}\left(\log_2\left(1+\frac{N_1}{D_1}\right) - \frac{1}{\ln 2}\int_0^\infty \frac{1}{1+\upsilon} \right.$$

$$\left.\left(1-\exp\left\{-\frac{\lambda_e}{\alpha}\underbrace{\exp\left\{-\Delta|c_{4,k}|^2\upsilon\right\}}_{A}\underbrace{(\Delta\upsilon)^{-2/\alpha}}_{B}\left[\underbrace{\pi\Gamma\left(\frac{2}{\alpha}\right)+\int_{\pi/2}^{3\pi/2}\Gamma\left(\frac{2}{\alpha},\Delta\upsilon\left(-2R_0\cos\theta\right)^{\alpha}\right)\mathrm{d}\theta}_{C}\right]\right\}\right)\mathrm{d}\upsilon\right)^{+} \tag{27}$$

$$f(\rho) = -\frac{1}{\ln 2}\frac{\sigma_{n_d}^2 c_5 N_1/(1-\rho)}{(D_1+N_1)\,D_1} - \frac{1}{\ln 2}\frac{\lambda_e}{\alpha}\int_0^{\upsilon_{\mathrm{th}}}\frac{1}{1+\upsilon}\exp\left\{-\frac{\lambda_e}{\alpha}ABC\right\}\left(\frac{1}{\alpha}ABD+\left(AE+\frac{1}{\alpha}FB\right)C\right)\mathrm{d}\upsilon \tag{30}$$

$$D = -1/(1-\rho)\int_{\pi/2}^{3\pi/2}\exp\left\{-\Delta\upsilon(-2R_0\cos(\theta))^{\alpha}\right\}\left(\Delta\upsilon(-2R_0\cos(\theta))^{\alpha}\right)^{2/\alpha}\mathrm{d}\theta \tag{31}$$

$$F = -\Delta\upsilon\exp\{-\Delta|c_4|^2\upsilon\}\left(\eta(1-\rho)P_sA_0^2\beta_{sr}^{-\alpha}\sum_{i=1}^{N}\alpha_i/\sigma_{n_e}^2\right) \tag{32}$$

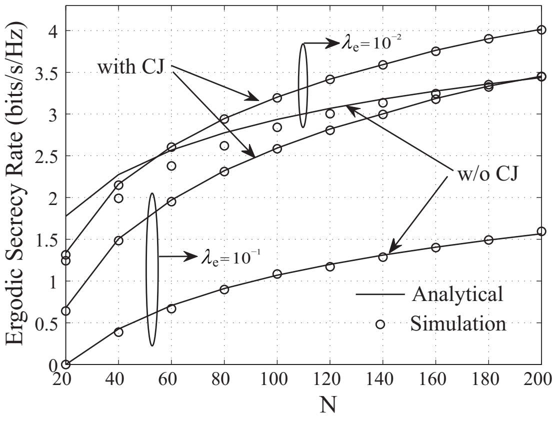

Fig. 2. The asymptotic ergodic secrecy rate by the proposed AF relaying vs the number of relay antennas, P_s = 30dBm, $\alpha = 2.5$, and $R_0 = 13.33$m.

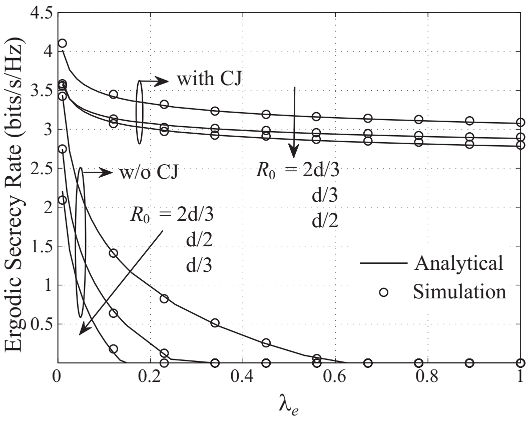

Fig. 3. The asymptotic ergodic secrecy rate by the proposed AF relaying vs eavesdroppers' density, P_s = 30dBm, $\alpha = 2.5$, and $N = 200$.

IV. Numerical Results

In this section, we provide numerical results to validate the proposed CJ-aided wireless powered AF relaying against the benchmark scheme, "w/o CJ", in which ρ is fixed as zero. The destination is assumed to be a total d = 20m far from the source, while the AF relay is set on the source-destination link with a distance of R_0 from the source ($d - R_0$ from the destination). The eavesdroppers are deployed as HPPP excluded from a "security zone" as stated in Section II. The involved channels are modelled with all the relevant distances referred to the relay as the origin. Unless otherwise specified, d_0 = 1m, $\eta = 0.5$, $\alpha = 2.5$, P_s = 30dBm, $\sigma_{n_a}^2 = -110$dBm, and $\sigma_{n_c}^2 = -70$dBm. The average AWGN power at all the nodes are set to be the same as $\sigma_{n_a}^2 + \sigma_{n_c}^2$.

In Fig. 2 and Fig. 3, analytical results are obtained from the asymptotic ergodic secrecy rate in (27) using the optimal power allocation factor ρ^* in (29), while the simulation points are plotted from the exact ergodic secrecy rate in (24). We see that the simulation points are in precise agreement with the analytical results of the asymptotic ergodic secrecy rate at large N (e.g., $N = 160$), which validates our analysis.

Fig. 2 shows the asymptotic ergodic secrecy rate versus the number of relay antennas N. As expected, the ergodic secrecy rate increases with N, which results from the array again brought by using MRT and MRC at the relay. For the given density of eavesdroppers, the ergodic secrecy rate with CJ using ρ^* always outperforms that w/o CJ (see the simulation points obtained by the exact ergodic secrecy rate) especially in the situation of larger eavesdroppers' density λ_e, which reveals the considerable improvement on the ergodic secrecy rate with the aid of CJ when the number of relay antennas is very large.

Fig. 3 depicts the asymptotic ergodic secrecy rate versus the density of eavesdroppers λ_e. We see that the ergodic secrecy rate goes down with the increasing λ_e due to the increasing chance of a very large $\mathrm{SINR}_{re,k}$. For the benchmark scheme w/o CJ, the ergodic secrecy rate increases with the AF relay located closer to the destination as a result of improvement on the main channel's capacity. Moreover, for the "with CJ" scheme, the maximum shown ergodic secrecy rate is also achieved with the shortest distance to the destination from the relay (i.e., $R_0 = 2d/3$), the behaviour of which is surprisingly immune to the nevertheless longer WPT distance from the source thanks to the large N. The obviously noticeable performance gain by "with CJ" with λ_e up to 1, further demonstrates the significance of CJ-aided cooperation design in safeguarding the PLS.

V. Conclusion

In this work, we studied the impact of MRC and MRT based AF relay beamforming and CJ on the ESR for cooperative secrecy transmission via a large-number-antenna equipped WEH-enabled relay. Assuming full CSI of the legitimate channel and no CSI of the eavesdropping channel, the ESR was characterized by eavesdroppers' spatial distribution density using stochastic geometry tools. The analytical results were asymptotically achieved by simulations when the number of relay antennas was vary large. In addition, the proposed cooperation scheme with optimum power allocation for CJ was shown to be prominently robust against an unknown number of densely located eavesdroppers.

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[2] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[3] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[4] S. Bi, Y. Zeng, and R. Zhang, "Wireless powered communication networks: An overview," *to appear in IEEE Wireless Commun. Mag.*, 2015, available online at arXiv:1508.06366.

[5] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[6] H. Xing, K.-K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: a paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616–6631, Dec. 2015.

[7] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.

[8] G. Yang, C. K. Ho, R. Zhang, and Y. L. Guan, "Throughput optimization for massive MIMO systems powered by wireless energy transfer," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 8, pp. 1640–1650, Aug. 2015.

[9] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sept. 2014.

[10] 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.

[11] Y. Deng, L. Wang, K.-K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, "Safeguarding massive mimo aided hetnets using physical layer security," in *Int. Wireless Commun. Signal Process. (WCSP)*, Oct. 2015, pp. 1–5.

[12] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Aritificial-noise aided secure transmission in large scale spectrum sharing networks," *to appear in IEEE Trans. Commun.*, 2016.

[13] A. Nasir, X. Zhou, S. Durrani, and R. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, July 2013.

[14] M. Zhao, X. Wang, and S. Feng, "Joint power splitting and secure beamforming design in the multiple non-regenerative wireless-powered relay networks," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1540–1543, Sept. 2015.

[15] H. Xing, K.-K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *submitted to IEEE Trans. Wireless Commun.*, available online at arXiv:1511.03705.

[16] X. Chen, J. chen, and T. Liu, "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization," *to appear in IEEE Trans. Veh. Technol.*, 2015.

[17] A. Jeffrey and D. Zwillinger, *Table of Integrals, Series, and Products*. Academic Press, 2007.

[18] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[19] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 996–1019, 3rd Quart. 2013.

[20] A. Hasan and J. G. Andrews, "The guard zone in wireless ad-hoc networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 897–906, Mar. 2007.

[21] O. Klesov, *Limit Theorems for Multi-Indexed Sums of Random Variables*, ser. Probability Theory and Stochastic Modelling. Berlin, Germany: Springer, 2014, vol. 71.

[22] H. Deng, H. M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.