Exploiting Jamming Attacks for Energy Harvesting in Massive MIMO Systems

Hayder Al-Hraishawi, Symeon Chatzinotas, and Björn Ottersten
Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg.
emails: {hayder.al-hraishawi, symeon.chatzinotas, bjorn.ottersten}@uni.lu

***Abstract*—In this paper, the performance of an RF energy harvesting scheme for multi-user massive multiple-input multiple-output (MIMO) is investigated in the presence of multiple active jammers. The key idea is to exploit the jamming transmissions as an energy source to be harvested at the legitimate users. To this end, the achievable uplink sum rate expressions are derived in closed-form for two different antenna configurations. An optimal time-switching policy is also proposed to ensure user-fairness in terms of both harvested energy and achievable rate. Besides, the essential trade-off between the harvested energy and achievable sum rate are quantified in closed-form. Our analysis reveals that the massive MIMO systems can make use of RF signals of the jamming attacks for boosting the amount of harvested energy at the served users. Numerical results illustrate the effectiveness of the derived closed-form expressions over Monte-Carlo simulations.**

I. Introduction

Mobile and IoT devices in beyond 5G technologies will fundamentally be empowered by artificial intelligence (AI) processing, which makes them more power hungry due to the high computational loads [1]. Meanwhile, energy harvesting from ambient radio frequency (RF) signals has emerged as a sustainable solution for the tremendous growth in the energy consumption of wireless networks. Moreover, as wireless network densification continues and communication distance is becoming much shorter, wireless energy harvesting will be more meaningful for the applications with limited-capacity power sources. However, there are some practical limitations inhibit harvesting enough energy at the receivers such as the low RF energy to direct current (DC) conversion efficiency and the severe path-loss between the transmitter and the receiver. To this end, smart antennas technologies such as massive MIMO can be used to enhance the performance of energy harvesting and then boost the overall energy efficiency and achievable data rate [2].

Massive MIMO as a concept accommodates the massive connectivity requirement that is essential for future wireless cellular networks to support IoT and machine-type communications (MTC) [3], [4]. Nevertheless, universal wireless connectivity is appealing to the envisioned beneficiaries of these networks as well as to the bad actors where they can wreak havoc by actively eavesdropping and jamming. Moreover, jamming devices used to be implemented on expensive hardware mostly for military purposes, but currently it is possible to obtain a jamming device by modifying the firmware of commodity hardware [5]. Additionally, active jammers need a sufficiently high energy budget for each transmission block, which is allocated between pilot spoofing attacks during channel training phase and jamming the legitimate communications during data transmission phase [6]. Accordingly, different from other works in the context of energy harvesting, we consider utilizing the jamming energy transmitted by the active eavesdroppers to be harvested at the legitimate users.

Towards detecting the jamming threats, there have been abundant research works with various effective approaches proposed. Specifically, the authors in [7] have conducted a survey on the methods that detect active attacks on massive MIMO systems. On the other hand, jamming defense strategies for massive MIMO are developed in [8] in which secret keys are employed to encrypt and protect the legitimate communications from the jamming attacks. In [9], a jamming-resistant receiver scheme has been proposed to utilize the high spatial resolution of massive MIMO for enhancing the robustness of uplink transmissions. Moreover, the multi-antenna base-station (BS) can be used in such scenarios for provisioning physical layer security by exploiting the large antenna arrays to simultaneously transmit confidential signals towards the legitimate user nodes and artificial noise (AN) sequences towards eavesdroppers for perturbing their intercepted signals, and hence, improving the secrecy performance.

Furthermore, the security aspects of massive MIMO systems with the presence of active and passive eavesdroppers have been extensively studied in multiple works [9]–[14]. For instance, reference [14] investigates an AN-aided transmitter for secure communications in the presence of attackers capable of both jamming and eavesdropping. Nevertheless, we will not delve into similar mechanisms that aiming at strengthening the security or incapacitating the eavesdropper's ability to decode the confidential data, which are beyond the scope of this work. Instead, we focus on exploiting the jamming signals of the active attackers as a viable source for energy harvesting, and thus, increasing the energy efficiency of massive MIMO networks. Specifically, the objective of this paper is to make full use of the RF energy in wireless environment.

The concept of energy harvesting has been widely adopted in massive MIMO systems, where some of the prior related works can be outlined as follows: in [15] an energy harvesting strategy has developed and analyzed to power the secondary users of a cognitive radio system through harvesting energy from primary user transmissions. Reference [16] has proposed and analyzed an architecture of self-backhaul and energy harvesting small cell network with massive MIMO. In

[17], the trade-off between the achievable rate and harvested energy has been analyzed at massive MIMO receivers, where a low-complexity antenna partitioning algorithm for energy harvesting massive MIMO systems is proposed. Additionally, in a secrecy transmission over a multi-user MIMO system, an AN-injection scheme has been employed to mask the desired information signals for secrecy consideration while the severed users harvest energy from both the information-bearing signal and the AN [18]. Throughout the open literature, exploiting the transmissions of the jammers as an energy source has not been investigated yet. Therefore, this observation motivates this work to study the performance of a massive MIMO system utilizes the jammer attacks to power the legitimate users.

The main technical contributions of this work can be summarized as follows: A novel RF energy harvesting scheme for massive MIMO has been proposed to fully utilize the RF energy in wireless environments. Specifically, the legitimate user nodes can harvest energy from the jamming transmissions of the active attackers in order to utilize this energy for sending their payload data to the BS. To the best of our knowledge, this has not been done in the existing studies in the literature. We consider the uplink transmission since we want evaluate the achievable data rate by the users when the proposed energy harvesting scheme is employed. The basic performance metrics of the proposed energy-harvesting scheme are derived for finite/infinite antenna regime at the BS with taking into account the cumulative impact of imperfect channel state information (CSI) and co-channel interference. The achievable uplink data rate is derived based on the worst-case Gaussian technique for the case of finitely many antennas at the BS. This technique is practically useful when the instantaneous CSI is not available.

The rest of the paper is structured as follows. The considered system model is presented in Section II. Next, the performance metrics are derived for both limited and unlimited antenna arrays at the BS in Section III. Numerical results and discussions on our proposed scheme are provided in Section IV. Finally, Section V summarizes the concluding remarks.

Notation: $\mathbf{Z}^H$ and $[\mathbf{Z}]_{i,j}$ denote the Hermitian-transpose and the (i,j)th element of the matrix $\mathbf{Z}$, respectively. The absolute value and norm operator are denoted by $|\cdot|$ and $\|\cdot\|$, respectively. $\mathbb{E}[z]$ and $\mathbb{V}\mathrm{ar}[z]$ are the expected value and the variance of z, and the operator $\otimes$ denotes the Kronecker product. $\mathrm{Ei}(z)$ is the exponential integral function for the positive values of the real part of z. Finally, the notation $\mathbf{Z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma})$ denotes that $\mathbf{Z}$ is a circularly symmetric complex Gaussian distributed with zero mean and covariance matrix $\mathbf{\Sigma}$.

II. System, channel, and signal models

A. System and channel models

We consider the uplink transmission of a multi-user MIMO network that consists of an M-antennas BS to serve K randomly distributed user nodes (U_k) for $k \in \{1, \cdots, K\}$ in the presence of N randomly located active jammers (J_n) for $n \in \{1, \cdots, N\}$. Each user node and jammer is herein assumed to be equipped with a single antenna as shown in Fig. 1. This model captures the key idea of jamming multiple concurrent communications and our analysis can be readily generalized to the case of multi-cell systems.

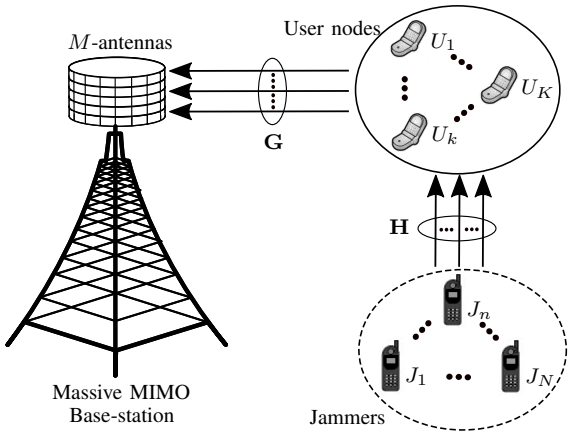

Fig. 1. Massive MIMO uplink transmissions under jamming attacks.

Let $\mathbf{G} \in \mathbb{C}^{(M \times K)}$ be the channel matrix between the BS and user nodes, which can be modeled as

$$\mathbf{G} = \tilde{\mathbf{G}} \mathbf{D}_G^{1/2}, \tag{1}$$

where $\tilde{\mathbf{G}} \sim \mathcal{CN}_{M \times K}(\mathbf{0}_{M \times K}, \mathbf{I}_M \otimes \mathbf{I}_K)$ accounts for the independent small-scale Rayleigh fading, and diagonal matrix $\mathbf{D}_G = \mathrm{diag}(\zeta_{G_1}, \cdots, \zeta_{G_k}, \cdots, \zeta_{G_K})$ captures the large-scale fading including path-loss and shadowing.

User nodes can harvest energy from the jamming transmissions of the active eavesdroppers through the jamming channel $\mathbf{H}$, which can be defined as

$$\mathbf{H} = \tilde{\mathbf{H}} \mathbf{D}_H^{1/2}, \tag{2}$$

where $\tilde{\mathbf{H}} \sim \mathcal{CN}_{K \times N}(\mathbf{0}_{K \times N}, \mathbf{I}_K \otimes \mathbf{I}_N)$ captures the independent small-scale Rayleigh fading channel, and $\mathbf{D}_H$ accounts the energy harvesting channel large-scale fading. Here, the elements of $\mathbf{D}_H$ can be vectorized as $\mathrm{vec}[\mathbf{D}_H] = [\beta_{H_{11}}, \cdots, \beta_{H_{1N}}, \cdots, \beta_{H_{KN}}]$.

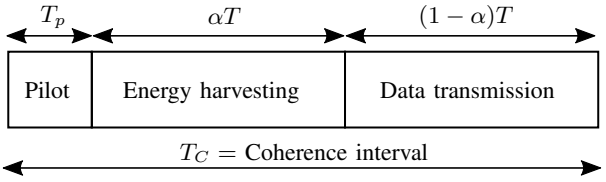

Fig. 2. Transmission frames for users, where $T = T_C - T_p$.

A block-fading model has been considered in this analysis, where the channel remains constant during a coherence block of T_C symbol times, which is practically computed as the product of the coherence time and the coherence bandwidth. Signals consisting of T_C symbols can be transmitted in a coherence block and these signals can be represented by vectors of T_C lengths. Specifically, the considered massive MIMO system is operating in time-division duplex (TDD) mode, and the uplink transmission coherence block (T_C) of each user node is divided into three orthogonal time-slots as depicted in Fig. 2. At the beginning of each coherence

block, all user nodes simultaneously transmit orthogonal pilot sequences during (T_p) to the BS for estimating their respective channels. Afterwards, user nodes harvest energy during αT, where $\alpha \in (0,1)$ is the time-switching factor and $T = T_C - T_p$. The user nodes utilize the harvested energy for data transmission during the remaining time duration $(1-\alpha)T$. Meanwhile, we assume that the active jammers are constantly transmitting to jam the user nodes.

B. Acquisition of channel state information

In practice, the channels are estimated during the uplink channel training phase (T_p) at the BS through uplink pilot sequences transmitted by the user nodes. Then, these uplink channel estimates are used by the BS to obtain the downlink channels via channel reciprocity that holds in TDD systems [19]. Specifically, at the beginning of the channel training phase, all user nodes transmit their pilot sequences $\mathbf{\Phi}_k \in \mathbb{C}^{(1\times T_p)}$, where T_p is the pilot sequence length, satisfying $T_p \geq K$. Furthermore, $\mathbf{\Phi}_k \mathbf{\Phi}_k^H = 1$ and $\mathbf{\Phi}_k \mathbf{\Phi}_{k'}^H = 0$ when $k \neq k'$ and $k, k' \in \{1, \ldots, K\}$. Accordingly, the pilot signal received at the BS can be written as

$$\mathbf{Y}_{\mathrm{p}} = \sum_{k=1}^{K} \sqrt{T_p \mathcal{P}_p}\, \mathbf{g}_k \mathbf{\Phi}_k + \mathbf{N}_{\mathrm{p}}, \tag{3}$$

where $\mathcal{P}_p$ is the average pilot transmit power of the user nodes, while $\mathbf{N}_{\mathrm{p}}$ is an additive white Gaussian noise (AWGN) matrix whose elements are independent and identically distributed (i.i.d.) $\mathcal{CN}(0,1)$ random variables. After projecting $\mathbf{Y}_{\mathrm{p}}$ onto $\mathbf{\Phi}_k$, the minimum mean square error (MMSE) estimates of $\mathbf{g}_k$ can be derived as [20]

$$\hat{\mathbf{g}}_k = \sqrt{T_p \mathcal{P}_p}\zeta_{G_k} (1 + T_p \mathcal{P}_p \zeta_{G_k})^{-1}\, \mathbf{Y}_{\mathrm{p}} \mathbf{\Phi}_k \tag{4}$$

The MMSE estimate of $\hat{\mathbf{G}}$ can be then written as $\hat{\mathbf{G}} = [\hat{\mathbf{g}}_1; \cdots; \hat{\mathbf{g}}_k; \cdots; \hat{\mathbf{g}}_K]$. The true channel of $\mathbf{G}$ can be written in terms of its estimate as

$$\mathbf{G} = \hat{\mathbf{G}} + \boldsymbol{\mathcal{E}}_G \tag{5}$$

where $\boldsymbol{\mathcal{E}}_G$ is the channel estimation error matrix. From the orthogonality property of MMSE, $\hat{\mathbf{G}}$ and $\boldsymbol{\mathcal{E}}_G$ are statistically independent and distributed as $\hat{\mathbf{G}} \sim \mathcal{CN}(0, \hat{\mathbf{D}}_G)$ and $\boldsymbol{\mathcal{E}}_G \sim \mathcal{CN}(0, \mathbf{D}_G - \hat{\mathbf{D}}_G)$, respectively, where $\hat{\mathbf{D}}_G$ is a diagonal matrix with the k-th diagonal element is given by $\hat{\zeta}_{G_k} = T_p \mathcal{P}_p \zeta_{G_k}^2 (1 + T_p \mathcal{P}_p \zeta_{G_k})^{-1}$.

C. Energy harvesting

During the second portion of uplink time-slot having a length of αT, user nodes harvest energy from the jamming transmissions. Thus, the average harvested energy at the k-th user can be expressed as

$$E_{h_k} = \eta \alpha T \left\| \mathbf{h}_k \mathbf{P}_E^{1/2} \right\|^2, \tag{6}$$

where $\mathbf{P}_E = \mathrm{diag}(P_{E_1}, \cdots, P_{E_n}, \cdots, P_{E_N})$ accounts for the jamming powers of the active attackers for $n \in \{1, \cdots, N\}$, $\mathbf{h}_k$ is the k-th row of $\mathbf{H}$, η is the RF-to-DC conversion efficiency.

User nodes utilize the harvested energy in (6) for transmitting their payload data to the BS during the remaining time duration $(1-\alpha)T$, and thus, the uplink transmission power of the k-th user node can be defined as

$$P_{d_k} = E_{h_k} / (1-\alpha) T. \tag{7}$$

D. Signal model for uplink transmission

In this subsection, the signal model for the massive MIMO uplink transmission is presented. Thus, the received signal at the BS after applying the zero-forcing[1] (ZF) detector can be written as

$$\mathbf{y}_U = \hat{\mathbf{W}} \left(\sqrt{\mathbf{P}_d} \mathbf{G} \mathbf{x}_d + \mathbf{n}_U \right), \tag{8}$$

where $\hat{\mathbf{W}}$ is the ZF detector at the BS and is defined as

$$\hat{\mathbf{W}} = (\hat{\mathbf{G}}^H \hat{\mathbf{G}})^{-1} \hat{\mathbf{G}}^H. \tag{9}$$

In (8), $\mathbf{P}_d = \mathrm{diag}(P_{d_1}, \cdots, P_{d_k}, \cdots, P_{d_K})$ is an $K \times K$ diagonal matrix representing the uplink transmit power for the K user nodes that obtained from (7) for $k \in \{1, \cdots, K\}$. Further, $\mathbf{x}_d$ is the transmitted vectors of the user nodes that satisfying $\mathbb{E}[\mathbf{x}_d \mathbf{x}_d^H] = \mathbf{I}_K$, and $\mathbf{n}_U \sim \mathcal{CN}(0,1)$ is the AWGN at the BS satisfying that $\mathbb{E}[\mathbf{n}_U \mathbf{n}_U^H] = \mathbf{I}_{n_U} \sigma_n^2$.

III. Performance Analysis

In this section, the achievable uplink sum rates are derived for two different antenna configurations at the BS.

A. Uplink sum rate for finite number of BS antennas (M)

In order to capture the joint impact of detection uncertainty, interference, and filtered AWGN, the k-th user data stream received at the BS is written by using (8) as [19]

$$\tilde{y}_k = \sqrt{P_{d_k}} \mathbb{E}\left[\hat{\mathbf{w}}_k \mathbf{g}_k \right] x_{d_k} + \tilde{n}_{U_k} \tag{10}$$

where the first term accounts for the desired signal, and the second term represents the effective noise capturing the collective impacts of interference arises from detection uncertainty with imperfect CSI, inter-user interference, and filtered AWGN, which is expressed as

$$\begin{aligned} \tilde{n}_{U_k} =& \sqrt{P_{d_k}} \left(\hat{\mathbf{w}}_k \mathbf{g}_k - \mathbb{E}\left[\hat{\mathbf{w}}_k \mathbf{g}_k \right] \right) x_{d_k} \\ &+ \sum_{k=1, k' \neq k}^{K} \sqrt{P_{d_{k'}}} \hat{\mathbf{w}}_k \mathbf{g}_{k'} x_{d_{k'}} + \hat{\mathbf{w}}_k n_{U_k}. \end{aligned} \tag{11}$$

An achievable uplink sum rate expression, that can tightly bound the ergodic sum rate, is derived by invoking the worst-case Gaussian approximation technique as follows [19]

$$\mathcal{R}_U = \frac{(1-\alpha)T}{T_C} \sum_{k=1}^{K} \log_2 \left(1 + \tilde{\gamma}_k \right), \tag{12}$$

where $\tilde{\gamma}_k$ is the effective signal-to-interference-plus-noise ratio (SINR) of the k-th user node and is obtained as follows

$$\tilde{\gamma}_k = \frac{P_{d_k} \left| \mathbb{E}\left[\hat{\mathbf{w}}_k \mathbf{g}_k \right] \right|^2}{\mathrm{BU}_k + \sum\limits_{k'=1, k' \neq k}^{K} \mathrm{UI}_{kk'} + \sigma_n \mathbb{E}\left[\left\| \hat{\mathbf{w}}_k \right\|^2 \right]}, \tag{13}$$

[1]ZF-type receiver filter performs better than matched-filter detector in terms of nulling the jamming signal [9] and inter-pair interference mitigation [19].

where BU_k and $\mathrm{UI}_{kk'}$ are the beamforming gain uncertainty and the interference caused by other users, respectively, which can be defined as

$$\mathrm{BU}_k = P_{d_k} \mathbb{V}\mathrm{ar}\left[\hat{\mathbf{w}}_k \mathbf{g}_k\right], \tag{14a}$$

$$\mathrm{UI}_{kk'} = P_{d_{k'}} \mathbb{E}\left[\left|\hat{\mathbf{w}}_k \mathbf{g}_{k'}\right|^2\right]. \tag{14b}$$

Then, by evaluating the expectation and variance terms in (13), the achievable uplink sum rate for finite antenna regime at the BS can be derived in closed-form as follows (see Appendix A for the derivation)

$$\bar{\mathcal{R}}_U = \frac{(1-\alpha)T}{T_C} \sum_{k=1}^{K} \log_2 \left(1 + \frac{P_{d_k}(M-K)\hat{\zeta}_{G_k}}{\sum\limits_{k'=1}^{K} P_{d_{k'}}(\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}) + \sigma_n^2}\right). \tag{15}$$

B. Uplink sum rate for infinite number of antennas ($M \to \infty$)

In this subsection, the asymptotic uplink sum rate is derived when the number of antennas at the BS grows unbounded with respect to the number of served user nodes, i.e., the number of users (K) is kept at arbitrary finite value against M. Thus, the transmit power at the user nodes can be scaled inversely proportional to the number of antennas at the BS as $P_d = E_d/M$, where E_d is constant. Then, by letting $M \to \infty$ in (15) and by invoking (7), the asymptotic SINR of the k-th user node can be derived as

$$\tilde{\gamma}_k^{\infty} = \frac{\eta\alpha\hat{\zeta}_{G_k}}{(1-\alpha)\sigma_n^2} \left\|\mathbf{h}_k \mathbf{P}_E^{1/2}\right\|^2 \tag{16}$$

Next, by using (16), the achievable uplink sum rate at the BS can be derived as (see Appendix B for the derivation).

$$\bar{\mathcal{R}}_U^{\infty} = \frac{(1-\alpha)}{\ln(2)} \sum_{k=1}^{K}\sum_{j=1}^{N} \Omega_j \left[-e^{\left(\mathcal{A}_k \beta_{H_j} P_{E_j}\right)^{-1}} \mathrm{Ei}\left(\frac{-1}{\mathcal{A}_k \beta_{H_j} P_{E_j}}\right)\right] \tag{17}$$

where $\mathcal{A}_k = \eta\alpha\hat{\zeta}_{G_k}/(1-\alpha)\sigma_n^2$, Ω_j is given in (28), and $\mathrm{Ei}(\cdot)$ is the exponential integral function [21].

Remark 1: The uplink sum rate and the harvested energy are increasing functions of N, and consequently, massive MIMO systems can take advantage of the jamming attacks for boosting their achievable rate, while evidently maintaining the secrecy performance through some secure communication techniques.

C. Optimization of time-switching factor

In this subsection, we will show that the time-switching factor can be optimized for jointly guaranteeing the user-fairness in terms of the harvested energy and achievable uplink rate of the user nodes. Based on the maximum fairness criterion, a max-min optimization problem can be formulated by first setting the user SINR targets equal to a common SINR ($\bar{\gamma}_k$), and then searching for the maximum value of the common SINR as follows

$$\underset{\alpha\ \forall k}{\text{maximize}} \quad \bar{\gamma}_k \tag{18a}$$

$$\text{subject to} \quad \bar{\gamma}_k \Delta_k \geq P_{d_k}(M-K)\hat{\zeta}_{G_k}, \ \ \forall k, \tag{18b}$$

$$0 \leq \alpha \leq 1, \ \ \forall k, \tag{18c}$$

where $\Delta_k = \sum_{k'=1}^{K} P_{d_{k'}}(\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}) + \sigma_n^2$. Since the objective function in this optimization problem is a monomial and the constrains are posynomials, this is a geometric program which can be solved by using CVX tool for disciplined convex programming to find the optimal time-switching factor α^*.

D. Rate-energy trade-off

In time-switching protocol, the energy harvesting and data transfers take place in two orthogonal time-slots. Particularly, the harvested energy is a monotonically increasing function of α, while on the contrary the achievable uplink rate is a monotonically decreasing function of α. Then, the rate-energy trade-off can be obtained by first solving for α in (6) and then by substituting it into (15) as follows

$$\bar{\mathcal{R}}_U^* \approx \sum_{k=1}^{K} \left(\frac{T}{T_C} - \bar{E}_h \Big/ \left(\eta T_C \sum_{n=1}^{N} P_{E_n}\beta_{H_{kn}}\right)\right) \times \log_2\left(1 + \frac{\psi_{d_k}(M-K)\hat{\zeta}_{G_k}}{\sum_{k'=1}^{K}\psi_{d_{k'}}(\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}) + \sigma_n^2}\right), \tag{19}$$

where ψ_{d_k} is defined as

$$\psi_{d_k} = \frac{\bar{E}_h \eta \sum_{n=1}^{N} P_{E_n}\beta_{H_{kn}}}{\eta T \sum_{n=1}^{N} P_{E_n}\beta_{H_{kn}} - \bar{E}_h}. \tag{20}$$

Remark 2: The obtained energy-rate trade-off in (19) is optimal owing to the max-min user-fairness when setting the harvested energy targets of each user to a common value $\bar{E}_h$. Hence, the max-min optimal time-switching factor corresponding to any system operating point can be obtained through applying this optimal energy-rate trade-off.

Remark 3: Since users and jammers are spatially-distributed, both transmission and harvesting channels experience distinctive path-losses within a coherence block. Therefore, user fairness must be jointly guaranteed in terms of both energy and rate in order to overcome the near-far effects and attain optimal levels of harvested energy and data rate.

IV. Numerical Results

In this section, we numerically evaluate the performance of the proposed energy harvesting scheme. To capture the effect of practical transmission impairments, the channel pathloss is modeled as $[\mathrm{PL}]_{\mathrm{dB}} = \mathrm{PL}_0 + 10v\log d/d_0$, where d, d_0, PL_0 and v are defined as the distance between the user nodes and the BS, a reference distance, the pathloss at the reference distance, and the pathloss exponent, respectively. Specifically, the simulation parameters are set to $n = 2.3$, $d_0 = 100$ m, $d_G = 100-300$ m, $d_H = 100-500$ m, $\eta = 0.7$, $\sigma_n^2 = 0$ dBW, and $\mathcal{P}_P = 0$ dBW. The coherence time is set to $T_C = 1$ms having 196 symbols, pilot length is $T_p = K$ [19].

In Fig. 3, the average achievable user rate at the BS in the finite antenna regime is plotted against the jamming power by considering different numbers of active jammers (N). The analytical uplink rate curves are plotted by using (15), and are compared to the Monte-Carlo simulations of the uplink rate expression in (12). It can be readily seen that the achievable rate gradually increases when the jammers transmit

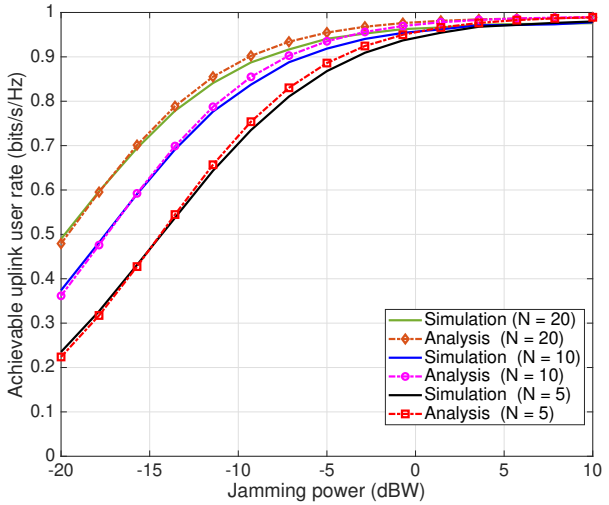

Fig. 3. Achievable uplink user rate for varying the jamming power when $K = 5$, $M = 20$, and $\alpha = 0.5$.

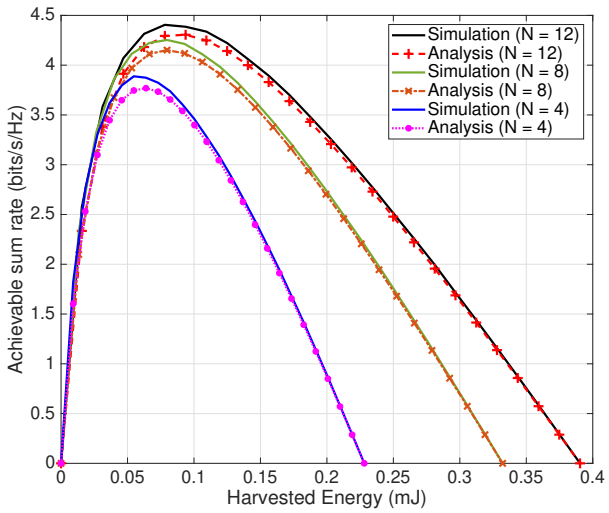

Fig. 4. Achievable sum rate versus the harvested energy for $K = 4$, $M = 15$.

higher power levels because the more jamming power, the greater energy will be harvested by the user nodes. Moreover, existence of fairly large number of jammers in the proximity of the served area can contribute to harvest more energy and eventually achieves higher data rate. Our analysis is compared against the Monte Carlo simulations to validate that the derived achievable rate by using the worst-case Gaussian technique provides a tight lower bound to the achievable rate.

Next, the relationship between the achievable sum rate at the BS and the harvested energy at the user nodes is investigated in the finite BS antenna regime and depicted in Fig. 4. We used the derived rate-energy trade-off expression in (19) to plot the analytical curves by considering different N. Clearly, the harvested energy increases with N, which leads to increased achievable sum rates due to the higher transmission powers of the user nodes. This observation validates the insights summarized in Remark 1, and Monte-Carlo simulations validate our analysis in (19).

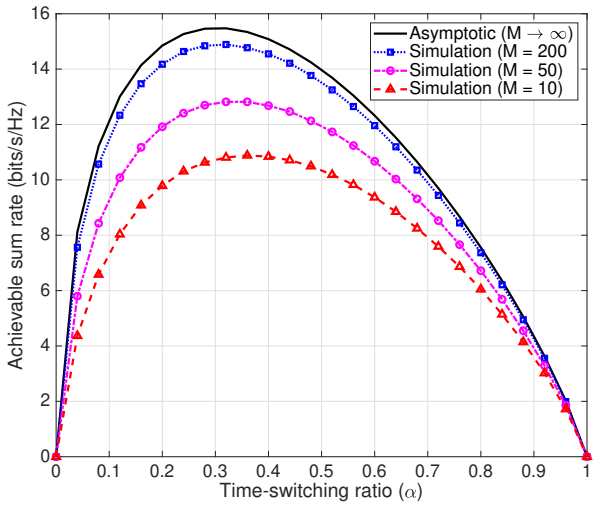

Fig. 5. Achievable uplink sum rate versus time-switching factor (α) for different M when $K = N = 5$.

In Fig. 5, the achievable uplink sum rate at the BS is plotted versus the time switching factor (α) by varying M. The asymptotic sum rate curves are plotted by using (17) and compared against the Monte-Carlo simulations. It can be seen that the sum rate approaches its maximum at the optimal α and then decreases after that. When α is small, the harvested energy by the user nodes is not sufficient to achieve high sum rate. However, a too large α value means more harvested energy but less residual time for the users' transmission, which also deteriorates the achievable sum rate. Fig. 5 reveals that the theoretical/asymptotic sum rate limits in (17) can be achieved when the number of BS antennas grows large.

V. Conclusion

The feasibility of exploiting the jamming transmissions of the active attackers for energy harvesting in massive MIMO system has been investigated. Towards this end, a wireless-powered multi-user massive MIMO system has been considered, where user nodes harvest energy from the jammers and utilize it for information transmission. System performance has been analyzed in training-based massive MIMO consisting of imperfectly estimated CSI at the BS and employing the time-switching protocol. The harvested energy, SINR, and sum rate expressions have been derived for finitely many BS antennas, where a tight sum rate expression is obtained in closed-form. The asymptotic performance metrics are also provided when the numbers of BS antennas grow without bound. Optimization of the time-switching factor has been formulated for jointly guaranteeing user-fairness in terms of both harvested energy and achievable rate of the spatially-distributed users. Our analysis concludes that adopting the proposed scheme in massive MIMO uplink transmissions for boosting the energy harvesting is practically feasible, and to validate this claim, the performance metrics have been analytically and numerically evaluated over different antenna configurations at the BS.

APPENDIX A
DERIVATION OF (15)

By using (5), the term $\hat{\mathbf{w}}_k\mathbf{g}_k$ can be simplified as follows:

$$\hat{\mathbf{w}}_k\mathbf{g}_k = \hat{\mathbf{w}}_k(\hat{\mathbf{g}}_k + \mathcal{E}_{G_k}) = 1 + \hat{\mathbf{w}}_k\mathcal{E}_{G_k}, \tag{21}$$

where $\mathcal{E}_{G_k}$ is the k-th column of estimation error matrix $\boldsymbol{\mathcal{E}}_G$. Since $\hat{\mathbf{w}}_k$ and $\mathcal{E}_{G_k}$ are uncorrelated and $\mathcal{E}_{G_k}$ is a zero-mean random variable, then $\mathbb{E}\left[\hat{\mathbf{w}}_k\mathcal{E}_{G_k}\right] = 0$. Therefore,

$$\mathbb{E}\left[\hat{\mathbf{w}}_k\mathbf{g}_k\right] = 1 + \mathbb{E}\left[\hat{\mathbf{w}}_k\mathcal{E}_{G_k}\right] = 1. \tag{22}$$

Next, the term accounts for the beamforming gain uncertainty BU_k can be derived by using (21) and (21) as

$$\begin{aligned}
\mathbb{V}\mathrm{ar}(\hat{\mathbf{w}}_k\mathbf{g}_k) &= \mathbb{E}\left[|\hat{\mathbf{w}}_k\mathcal{E}_{G_k}|^2\right] \\
&= (\zeta_{G_k} - \hat{\zeta}_{G_k})\mathbb{E}\left[\|\hat{\mathbf{w}}_k\|^2\right] \\
&= (\zeta_{G_k} - \hat{\zeta}_{G_k})\mathbb{E}\left[\left(\hat{\mathbf{G}}^H\hat{\mathbf{G}}\right)^{-1}\right]_{k,k} \\
&= \frac{(\zeta_{G_k} - \hat{\zeta}_{G_k})}{\hat{\zeta}_{G_k}K}\mathbb{E}[\mathrm{Tr}(\mathbf{X}^{-1})] \\
&= \frac{(\zeta_{G_k} - \hat{\zeta}_{G_k})}{\hat{\zeta}_{G_k}(M-K)},
\end{aligned} \tag{23}$$

where $\mathbf{X}$ is a $K \times K$ central Wishart matrix with N_P degrees of freedom and covariance matrix $\mathbf{I}_K$, where $\mathbb{E}[\mathrm{Tr}(\mathbf{X}^{-1})] = K/(M-K)$ [22].

The next term of the inter-user interference $\mathrm{UI}_{kk'}$ can be computed from (21), $\hat{\mathbf{w}}_k\mathbf{g}_{k'} = \hat{\mathbf{w}}_k\mathcal{E}_{G_{k'}}$ for $k' \neq k$. Since $\hat{\mathbf{w}}_k$ and $\mathcal{E}_{G_{k'}}$ are uncorrelated, then it can be shown that

$$\begin{aligned}
\mathbb{E}\left[|\hat{\mathbf{w}}_k\mathbf{g}_{k'}|^2\right] &= \left(\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}\right)\mathbb{E}\left[\left(\hat{\mathbf{G}}^H\hat{\mathbf{G}}\right)^{-1}\right]_{k,k} \\
&= \frac{\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}}{\hat{\zeta}_{G_k}(M-K)}.
\end{aligned} \tag{24}$$

Similarly, the noise term obtains as

$$\sigma_n^2\mathbb{E}\left[\|\hat{\mathbf{w}}_k\|^2\right] = \frac{\sigma_n^2}{\hat{\zeta}_{G_k}(M-K)}. \tag{25}$$

Then, by substituting (22), (23), (24), and (25) into (13), the achievable rate of the k-th at the BS can be derived as (15).

APPENDIX B
DERIVATION OF (17)

The obtained asymptotic SINR in (16) can be re-written as $\tilde{\gamma}_k^{\infty} = \mathcal{A}_k Z$, where $\mathcal{A}_k = \eta\alpha\hat{\zeta}_{G_k}/(1-\alpha)\sigma_n^2$ and $Z = \left\|\mathbf{h}_k\mathbf{P}_E^{1/2}\right\|^2 = \sum_{j=1}^{N} Z_j$ is a sum of N independent random variables that are exponentially distributed with each element having the probability density function (PDF) in the following form

$$f_{Z_j}(x) = \exp\left(\frac{-x}{\beta_{H_j}P_{E_j}}\right)/\left(\beta_{H_j}P_{E_j}\right), \quad x \geq 0. \tag{26}$$

However, when all Z_js are independent but not identically distributed with distinct average powers, then the PDF of Z is given by [23]

$$f_Z(z) = \sum_{j=1}^{N}\frac{\Omega_j}{\beta_{H_j}P_{E_j}}\exp\left(\frac{-z}{\beta_{H_j}P_{E_j}}\right), \quad z \geq 0. \tag{27}$$

where

$$\Omega_j = \prod_{i=1, i\neq j}^{N}\frac{\beta_{H_j}P_{E_j}}{\beta_{H_j}P_{E_j} - \beta_{H_i}P_{E_i}}. \tag{28}$$

Thus, the average sum rate can be written as

$$\bar{\mathcal{R}}_k^{\infty} = (1-\alpha)\sum_{k=1}^{K}\int_0^{\infty}\log_2\left(1 + \mathcal{A}_k z\right) f_Z(z)dz, \tag{29}$$

by evaluating this integral using [21], the achievable sum rate can be expressed as shown in (17).

REFERENCES

[1] F. Tariq *et al.*, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, 2020.

[2] Z. Ding *et al.*, "Application of smart antenna technologies in simultaneous wireless information and power transfer," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 86–93, 2015.

[3] L. Liu and W. Yu, "Massive connectivity with massive MIMO–Part I: Device activity detection and channel estimation," *IEEE Trans. Signal Process.*, vol. 66, no. 11, pp. 2933–2946, 2018.

[4] H. Al-Hraishawi, G. A. Aruma Baduge, H. Q. Ngo, and E. G. Larsson, "Multi-cell massive MIMO uplink with underlay spectrum sharing," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 5, no. 1, pp. 119–137, 2019.

[5] M. Vanhoef and F. Piessens, "Advanced Wi-Fi attacks using commodity hardware," in *Proc. 30th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, New Orleans, LA, USA, Dec. 2014, pp. 256–265.

[6] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[7] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[8] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *IEEE Conf. on Commun. and Netw. Secur. (CNS)*, Philadelphia, PA, USA, 2015.

[9] T. T. Do, E. Bjornson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 210–223, Jan. 2018.

[10] H. Al-Hraishawi, G. Baduge, and R. Schaefer, "Artificial noise-aided physical layer security in underlay cognitive massive MIMO systems with pilot contamination," *Entropy*, vol. 19, no. 7, p. 349, Jul 2017.

[11] H. Al-Hraishawi, G. Amarasuriya, and R. F. Schaefer, "Secure communication in underlay cognitive massive MIMO systems with pilot contamination," in *IEEE Globel Comnun. Conf.*, Dec. 2017, pp. 1–7.

[12] D. Kudathanthirige and G. A. A. Baduge, "Effects of pilot contamination attacks in multi-cell multi-user massive MIMO relay networks," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 3905–3922, 2019.

[13] N. Akbar, S. Yan, A. M. Khattak, and N. Yang, "On the pilot contamination attack in multi-cell multiuser massive MIMO networks," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2264–2276, 2020.

[14] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, 2016.

[15] H. Al-Hraishawi and G. A. A. Baduge, "Wireless energy harvesting in cognitive massive MIMO systems with underlay spectrum sharing," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 134–137, Feb. 2017.

[16] L. Chen *et al.*, "Green full-duplex self-backhaul and energy harvesting small cell networks with massive MIMO," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3709–3724, Dec. 2016.

[17] H. Wang, W. Wang, X. Chen, and Z. Zhang, "Wireless information and energy transfer in interference aware massive MIMO systems," in *IEEE Globel Comnun. Conf.*, Dec. 2014, pp. 2556–2561.

[18] Z. Zhu *et al.*, "Beamforming and power splitting designs for AN-aided secure multi-user MIMO SWIPT systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2861–2874, Dec. 2017.

[19] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. Cambridge University Press, 2016.

[20] S. M. Kay, *Fundamentals of Statistical Signal Processing: Practical: Algorithm Development*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[21] I. Gradshteyn and I. Ryzhik, *Table of integrals, Series, and Products*, 7th ed. Academic Press, 2007.

[22] A. M. Tulino and S. Verdu, "Random matrix theory and wireless communications," *Foundations Trends Commun. Inf. Theory*, vol. 1, no. 1, pp. 1–128, Jun. 2004.

[23] J. Proakis, *Digital communications*, 4th ed. New York:McGraw-Hill, Inc., 2001.