

Energy Harvesting From Jamming Attacks in Multi-User Massive MIMO Networks

Hayder Al-Hraishawi¹, Senior Member, IEEE, Osamah Abdullah², Symeon Chatzinotas³, Fellow, IEEE, and Björn Ottersten⁴, Fellow, IEEE

Abstract—Fifth-generation (5G) and beyond communication systems offer new functionalities and significant performance improvements but that comes at the cost of tougher energy requirements on user devices. Addressing this issue while reducing the environmental impact of the substantial increase in energy consumption can be achieved through energy-neutral systems that operate using energy harvested from radio frequency (RF) transmissions. In this direction, this work examines the concept of utilizing an unconventional source for RF energy harvesting. Specifically, 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 by the legitimate users. To this end, the feasibility of this concept is studied via system performance analysis for a training-based massive MIMO encompasses imperfectly estimated channel state information (CSI) at the base-station and employing the time-switching protocol. In particular, the achievable uplink sum rate expressions are derived in closed-form for two different antenna configurations at the base-station. Two optimal time-switching schemes are also proposed based on maximum sum rate and user-fairness criteria. The essential trade-off between the harvested energy and achievable sum rate in time-switching protocol are quantified in closed-form as well. Our analysis reveals that the proposed energy harvesting scheme from jamming signals is viable and can boost massive MIMO uplink performance by exploiting the surrounding RF signals of the jamming attacks for increasing the amount of harvested energy at the served users. Finally, numerical results validate the theoretical analyses and the effectiveness of the derived closed-form expressions through simulations.

Index Terms—Energy efficiency, energy harvesting, jamming attacks, massive MIMO, multi-user networks.

I. INTRODUCTION

USER devices in beyond fifth-generation (5G) wireless communication systems will essentially be empowered by artificial intelligence (AI) processing capabilities, which

Manuscript received 3 January 2023; revised 6 April 2023 and 20 May 2023; accepted 22 May 2023. Date of publication 25 May 2023; date of current version 21 August 2023. This work was presented in part at IEEE International Conference on Communications (ICC), Montreal, QC, Canada, 2021 [DOI: 10.1109/ICC42927.2021.9500422]. The editor coordinating the review of this article was C. Mastroianni. (Corresponding author: Hayder Al-Hraishawi.)

Hayder Al-Hraishawi, Symeon Chatzinotas, and Björn Ottersten are with the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, 1855 Luxembourg City, Luxembourg (e-mail: hayder.al-hraishawi@uni.lu).

Osamah A. Abdullah is with the Ministry of Higher Education and Scientific Research, Baghdad 10065, Iraq.

Digital Object Identifier 10.1109/TGCN.2023.3280036

raises the energy requirements and makes users more power hungry due to the high computational loads [2]. 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. Energy harvesting from RF signals has been initially proposed as an alternative source of energy for low-power applications, such as wireless sensor networks, wireless charging systems, and wireless body area networks [3]. Moreover, the recent developments in receiver design [4] have made RF energy harvesting practically feasible. Energy harvesting provides long-lasting operation for the network and forgoes the external power cables and periodic battery replacements [5]. Therefore, incorporating energy harvesting technologies in communication systems can enable the establishment of energy-efficient networks, which can reduce operational costs and mitigate the environmental impact of communication infrastructure powered by non-renewable sources. As such, this technology has gained significant attention due to its potential to address the increasing concerns about the detrimental environmental consequences associated with operating the communication infrastructures using fossil fuel.

Since future wireless networks will be more densified and the communication distances are becoming much shorter, wireless energy harvesting will be more meaningful and feasible for the users within the applications that have limited power supplies [6]. 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. Towards this end, smart antennas technologies such as massive MIMO that can enhance the performance of energy harvesting and then boost the overall energy efficiency and achievable data rate [7]. Specifically, the large antenna arrays in massive MIMO systems can be used for increasing the lifetime of energy constrained wireless networks where the transmitted RF energy can be focused towards the nodes that need to be charged wirelessly, leading to an energy efficient solution compared to a single-antenna transmitter [8]. Furthermore, massive MIMO resource allocation can be formulated as an optimization problem in which the degrees of freedom in the antenna arrays and time are optimized for enhancing of the energy harvesting performance [9].

In RF energy harvesting networks, the RF sources are essentially classified into two categories (i) dedicated RF sources and (ii) ambient RF sources. Dedicated RF sources, such as

power beacons [10] and hybrid access point [11], deploy for a sole purpose of transmitting energy to user devices. Whilst, an RF signal that carries both information and power is referred to as an ambient RF source. However, from an implementation perspective, there is a key information-energy transmission trade-off in such networks, which has been studied in [4] and two practically viable receiver designs have been proposed, i.e., time switching receiver and power splitting receiver. For time switching structure, a receiving antenna periodically switches between the energy harvesting mode and receiving information mode, whereas in power splitting receiver, a passive power splitter is used at each receiver antenna, the received signal is divided into two separate signal streams, and then sends the signal components to the co-located information processor and energy harvester. Practically, deploying power splitting requires the passive power splitter at each receiving antenna, whereas time switching can be readily implemented by a simpler switcher, and thus, this work concentrates on the time switching-based energy harvesting receivers.

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 [12], 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 [9] has proposed and analyzed an architecture of self-backhaul and energy harvesting small cell network with massive MIMO. In [13], 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. Authors in [14] have investigated the feasibility of utilizing a relay-assisted massive MIMO to enhance the performance of simultaneous wireless information and power transfer (SWIPT) by leveraging the excess degrees-of-freedom offered by massive antenna arrays at the base-station. Optimizing the energy efficiency in millimeter-wave massive MIMO systems has been investigated in [15] where the massive MIMO base-station harvests electromagnetic energy from the environment employing SWIPT technology. Additionally, downlink transmission of massive MIMO with the support of SWIPT system based on a power-splitting scheme has been studied in [16] to maximize the system's energy efficiency using joint system-level optimization.

Furthermore, massive MIMO as a concept is developed to accommodate the massive connectivity requirement that is essential for future wireless cellular networks to support machine-type communications (MTC) and Internet of Things (IoT) devices [17], [18]. Nevertheless, ubiquitous 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/or jamming [19]. Moreover, jamming devices used to be implemented on high-cost hardware mostly for military purposes but currently they can be realized through modifying the firmware of commodity hardware [20]. Additionally, it should be noted that active jammers require a significant amount of energy budget for each transmission block to attack the legitimate

communications [21]. Interestingly, these high-power jamming signals can be exploited at the legitimate user devices for energy harvesting purposes. Specifically, different from the existing research works in the context of RF energy harvesting, this paper intends to investigate using the jamming energy transmitted by the jammers to be harvested by the users. The exploration of this concept aligns with the broader trend of investigating alternative energy sources and developing energy-efficient solutions for wireless networks. By harnessing energy from jamming transmissions, wireless networks can achieve energy-neutral or energy-efficient operation, which can result in improved system performance, extended device lifetime, and enhanced sustainability.

In the context of detecting the jamming threats, many effective approaches have been proposed in the literature to deal with the security challenges posed by jamming threats. In particular, a detailed survey article on the methods and techniques that are employed for detecting active attacks on massive MIMO systems can be found in [22]. On the other hand, jamming defense strategies for massive MIMO are developed in [23] in which secret keys are employed to encrypt and protect the legitimate communications from the jamming attacks. Likewise, a full-stack framework for detecting and suppressing jamming attacks in cell-free massive MIMO system is proposed in [24] to utilize the unused pilots for designing a jammer detector based on the likelihood functions of the measured signals. Moreover, based on game theory, a beam-domain jamming defense approach is developed in [25] for suppressing the malicious attacks on the downlink transmissions of the massive MIMO systems. In [26], a jamming-resistant receiver scheme has been proposed to utilize the high spatial resolution of massive MIMO for enhancing the robustness of uplink transmissions.

The multi-antenna massive MIMO base-station can be used 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 [27]. In this direction, the communication secrecy aspects of massive MIMO systems in the presence of active and passive attacks have been extensively studied in multiple works [26], [27], [28], [29], [30], [31]. Specifically, securing the millimeter-wave (mm-Wave) massive MIMO channels by exploiting the spatial sparsity of legitimate user's channel has been studied in [31]. The proposed security scheme in [31] is based on processing information data onto dominant angle components of the sparse channel, while AN is broadcast over the remaining non-dominant angles interfering only with the eavesdropper with a higher probability. Nevertheless, we will not delve into similar mechanisms that pursue strengthening the communication security or incapacitating the eavesdropper's ability to decode the confidential data, which are beyond the scope of this particular work. Instead, we focus on exploiting the jamming transmissions as a viable source for energy harvesting, and thus, increasing the energy efficiency of massive MIMO networks. Through this work, we aim to contribute to the development of more efficient and sustainable wireless

communication systems by exploring new and innovative approaches to energy harvesting.

Although jamming attacks can pose a threat to security of wireless communications, these attacks also present an unexplored opportunity to harvest additional signal power. The harvested energy can then be used as an additional source of power that can be used to enhance the uplink transmission and improve the overall system performance [1]. In this direction, the design of an energy-harvesting receiver under jamming attacks has been investigated in some prior works based on the premise that the detrimental interference can be harvested to increase the transmit power [32], [33], [34], [35]. Specifically, an energy-harvesting receiver for two-way orthogonal frequency division multiplexing (OFDM) systems under hostile jamming is designed to simultaneously process information and harvest energy from the received desired signals as well as the jamming interference through a power splitter [32]. In [33], the authors show that energy harvesting can be exploited for counteracting the jamming interference in a wireless secret key generation (SKG) system that consists of a pair of legitimate nodes and a malicious jammer. The authors in [34] have exploited the harmful jamming signals by considering them as a valuable energy source for harvesting by the legitimate users in a traditional interference alignment network. In the same context, a strategic interaction framework between a pair of legitimate user nodes and a jammer have been formulated as a zero-sum game in [35], and the analysis has demonstrated that the legitimate user are capable of neutralizing the jammer by appropriately tuning the transmit power and the energy harvesting duration. Nevertheless, to the best of our knowledge, this concept has not been studied yet in the open literature on a whole system level by considering multiple legitimate users attacked by multiple jammers. Therefore, this observation motivates this work to study the performance of a massive MIMO system utilizes the jamming attacks to power the legitimate users.

The key technical contributions of this study can be summarized as follows:

- Developing a novel RF energy harvesting scheme for massive MIMO to fully utilize the ambient RF signals. 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 base-stations.
- Formulating and deriving the performance metrics of the proposed energy-harvesting scheme for finite/infinite antenna regime at the base-station with considering the accumulative impact of the imperfect channel state information (CSI) and co-channel interference while the jammers are independent and non-identically distributed (i.n.i.d.). The uplink transmissions have been investigated in order to evaluate the achievable data rates by the users when the proposed energy harvesting scheme is employed.
- Designing two optimal time-switching energy harvesting control schemes for the users based on the sum rate maximization and max-min user-fairness criteria.

- Analyzing the energy-rate trade-off in the time-switching energy harvesting protocol, and deriving this interaction in a closed-form expression. Numerical/simulation results are presented to validate our analysis and to obtain system-design insights.

The rest of the paper is structured as follows. The considered system model is presented in Section II. The performance metrics for both limited and unlimited antenna arrays at the base-station alongside with optimization of time-switching factor and the energy-rate trade-off analysis are all derived and presented 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 $\mathbb{V}\text{ar}[z]$ are the expected value and the variance of z , and the operator \otimes denotes the Kronecker product. $\text{Ei}(z)$ 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

In this section, the system, channel, and signal models are presented in details along with analyzing the energy harvesting model in massive MIMO networks.

A. System and Channel Models

We consider the uplink transmission of a multi-user massive MIMO network that consists of an M -antennas base-station to serve K randomly distributed user nodes (U_k) for $k \in \{1, \dots, K\}$ in the presence of N randomly located active jammers (J_n) for $n \in \{1, \dots, N\}$ attempt to interfere with the reception of the users. This means that the jamming signals are specifically directed towards the users, with the aim of disrupting their ability to receive and interpret data correctly. To achieve their objective of disrupting the reception of the users, the jammers transmit jamming signals with increased signal power, which is the most common method used by jammers to interfere with wireless communication systems [36], [37]. 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.

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

$$\mathbf{G} = \tilde{\mathbf{G}}\mathbf{D}_G^{1/2}, \quad (1)$$

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 $\mathbf{D}_G = \text{diag}(\zeta_{G_1}, \dots, \zeta_{G_k}, \dots, \zeta_{G_K})$ 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

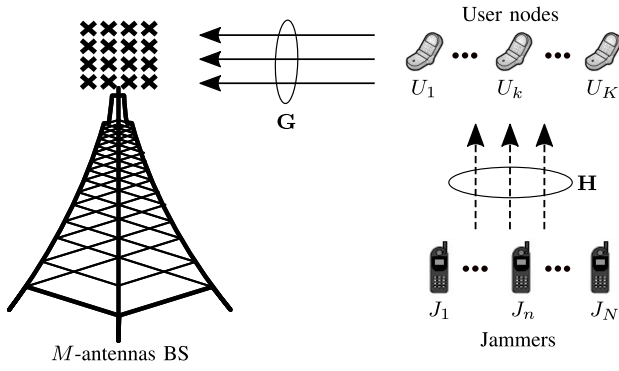


Fig. 1. Multi-user massive MIMO uplink transmissions under attacks by multiple jammers.

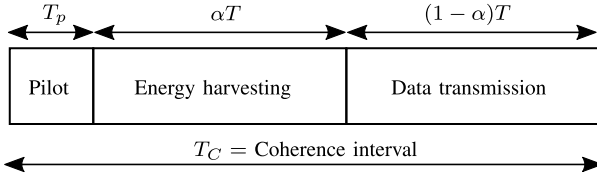


Fig. 2. A representation of a transmission frame in time-switching energy harvesting protocol for users, where $T = T_C - T_p$.

\mathbf{H} , which can be defined as

$$\mathbf{H} = \tilde{\mathbf{H}}\mathbf{D}_H^{1/2}, \quad (2)$$

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 $\text{vec}[\mathbf{D}_H] = [\beta_{H_{11}}, \dots, \beta_{H_{1N}}, \dots, \beta_{H_{KN}}]$.

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 represented in Fig. 2. At the beginning of each coherence block, all user nodes simultaneously transmit orthogonal pilot sequences during (T_p) to the base-station 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 base-station through uplink pilot sequences transmitted by the user nodes. Then, these uplink channel estimates are used by the base-station to

obtain the downlink channels via channel reciprocity that holds in TDD systems [38], [39]. Specifically, at the beginning of the channel training phase, all user nodes transmit their pilot sequences $\Phi_k \in \mathbb{C}^{(1 \times T_p)}$, where T_p is the pilot sequence length, satisfying $T_p \geq K$. Furthermore, $\Phi_k \Phi_k^H = \mathbf{1}$ and $\Phi_k \Phi_{k'}^H = 0$ when $k \neq k'$ and $k, k' \in \{1, \dots, K\}$. Accordingly, the pilot signal received at the base-station can be written as

$$\mathbf{Y}_p = \sum_{k=1}^K \sqrt{T_p \mathcal{P}_p} \mathbf{g}_k \Phi_k + \mathbf{N}_p, \quad (3)$$

where \mathcal{P}_p is the average pilot transmit power of the user nodes, while \mathbf{N}_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}_p onto Φ_k , the minimum mean square error (MMSE) estimates of \mathbf{g}_k can be derived as [40]

$$\hat{\mathbf{g}}_k = \sqrt{T_p \mathcal{P}_p} \zeta_{G_k} (1 + T_p \mathcal{P}_p \zeta_{G_k})^{-1} \mathbf{Y}_p \Phi_k^H \quad (4)$$

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

$$\mathbf{G} = \hat{\mathbf{G}} + \mathcal{E}_G \quad (5)$$

where \mathcal{E}_G is the channel estimation error matrix. From the orthogonality property of MMSE, $\hat{\mathbf{G}}$ and \mathcal{E}_G are statistically independent and distributed as $\hat{\mathbf{G}} \sim \mathcal{CN}(0, \hat{\mathbf{D}}_G)$ and $\mathcal{E}_G \sim \mathcal{CN}(0, \mathbf{D}_G - \hat{\mathbf{D}}_G)$, 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

Before deriving the achievable rate in the next Section III, we first obtain the harvested energy. 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 computed as

$$E_{h_k} = \alpha T \Psi_{EH_k}(P_{I_k}), \quad (6)$$

where P_{I_k} is the incident power at the rectenna of the k -th user and can be defined by as

$$P_{I_k} = \left\| \mathbf{h}_k \mathbf{P}_E^{1/2} \right\|^2, \quad (7)$$

where $\mathbf{P}_E = \text{diag}(P_{E_1}, \dots, P_{E_n}, \dots, P_{E_N})$ accounts for the jamming powers of the active attackers for $n \in \{1, \dots, N\}$, \mathbf{h}_k is the k -th row of \mathbf{H} .

Moreover, in (6), $\Psi_{EH_k}(\cdot)$ is a non-linear function of the incident power P_{I_k} . The practical non-linear energy harvesting model in [41] is considered in this analysis because practically the harvested energy is a non-linear function of the incident RF power at the rectenna. Typically, the RF-to-direct current (RF-to-DC) energy conversion efficiency increases with the incident power until a peak, and then it saturates to a constant defined by the characteristics of energy harvesting circuitry. This non-linear model contradicts the linear energy harvesting model that has been considered in multiple studies

as it largely overestimates the harvested energy in high incident power regime. The practically-viable non-linear operating characteristics of the energy harvesting circuitry is given in the following expression

$$\Psi(\rho) = \left[\frac{\delta}{1-v} \left(\frac{1}{1+e^{-\psi(\rho-w)}} - v \right) \right]^+, \quad (8)$$

where $[\lambda]^+ = \max(0, \lambda)$, $v = 1/(1 + e^{\psi w})$, and ρ is the incident power. The parameters δ , ψ , and w capture various non-linear effects of energy harvesting circuitry, and they can be defined for practical energy harvesters as $\delta = 9.079\mu W$, $\omega = 2.9\mu W$.

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

$$P_{d_k} = \frac{E_{h_k}}{(1 - \alpha)T}. \quad (9)$$

D. Signal Model for Uplink Transmission

This subsection considers modeling and analyzing the signal model for the massive MIMO uplink transmission. In particular, the received signal at the base-station after applying the zero-forcing¹ (ZF) detector can be written as

$$\mathbf{y}_U = \hat{\mathbf{W}} \left(\sqrt{\mathbf{P}_d} \mathbf{G} \mathbf{x}_d + \mathbf{n}_U \right), \quad (10)$$

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

$$\hat{\mathbf{W}} = \left(\hat{\mathbf{G}}^H \hat{\mathbf{G}} \right)^{-1} \hat{\mathbf{G}}^H. \quad (11)$$

In (10), $\mathbf{P}_d = \text{diag}(P_{d_1}, \dots, P_{d_k}, \dots, P_{d_K})$ is an $K \times K$ diagonal matrix representing the uplink transmit power for the K user nodes that obtained from (9) for $k \in \{1, \dots, K\}$. 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 base-station 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 base-station. This section also presents the optimization of the time-switching energy harvesting protocol in terms of maximum sum rate and user-fairness along with quantifying the trade-off between the harvested energy and uplink achievable rate.

A. Uplink Sum Rate for Finite Number of Base-Station Antennas

In order to capture the joint impact of detection uncertainty, interference, and filtered AWGN, the k -th user data stream received at the base-station is written by using (10) as

$$\tilde{y}_k = \sqrt{P_{d_k}} \mathbb{E}[\hat{\mathbf{w}}_k \mathbf{g}_k] x_{d_k} + \tilde{n}_{U_k}, \quad (12)$$

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

$$\begin{aligned} \tilde{n}_{U_k} = & \sqrt{P_{d_k}} (\hat{\mathbf{w}}_k \mathbf{g}_k - \mathbb{E}[\hat{\mathbf{w}}_k \mathbf{g}_k]) x_{d_k} \\ & + \sum_{k=1, k' \neq k}^K \sqrt{P_{d_{k'}}} \hat{\mathbf{w}}_{k'} \mathbf{g}_{k'} x_{d_{k'}} + \hat{\mathbf{w}}_k n_{U_k}. \end{aligned} \quad (13)$$

The achievable uplink sum rate can be tightly lower bounded by utilizing the use-and-then-forget bound in [39, Ch. 2], i.e., the worst-case Gaussian approximation technique:

$$R_U \geq \frac{(1 - \alpha)T}{T_C} \sum_{k=1}^K \log_2(1 + \tilde{\gamma}_k), \quad (14)$$

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

$$\tilde{\gamma}_k = \frac{P_{d_k} |\mathbb{E}[\hat{\mathbf{w}}_k \mathbf{g}_k]|^2}{\text{BU}_k + \sum_{k'=1, k' \neq k}^K \text{UI}_{kk'} + \sigma_n \mathbb{E}[\|\hat{\mathbf{w}}_k\|^2]}, \quad (15)$$

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

$$\text{BU}_k = P_{d_k} \mathbb{V} \text{ar}[\hat{\mathbf{w}}_k \mathbf{g}_k], \quad (16a)$$

$$\text{UI}_{kk'} = P_{d_{k'}} \mathbb{E}[|\hat{\mathbf{w}}_{k'} \mathbf{g}_{k'}|^2]. \quad (16b)$$

Next, the achievable uplink sum rate at the base-station can be derived in closed-form as follows. To begin with, the term $\hat{\mathbf{w}}_k \mathbf{g}_k$ in (5) can be simplified as follows:

$$\hat{\mathbf{w}}_k \mathbf{g}_k = \hat{\mathbf{w}}_k (\hat{\mathbf{g}}_k + \mathcal{E}_{G_k}) = 1 + \hat{\mathbf{w}}_k \mathcal{E}_{G_k}, \quad (17)$$

where \mathcal{E}_{G_k} is the k -th column of estimation error matrix \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 $\mathbb{E}[\hat{\mathbf{w}}_k \mathcal{E}_{G_k}] = 0$. Therefore,

$$\mathbb{E}[\hat{\mathbf{w}}_k \mathbf{g}_k] = 1 + \mathbb{E}[\hat{\mathbf{w}}_k \mathcal{E}_{G_k}] = 1. \quad (18)$$

Next, the term accounts for the beamforming gain uncertainty BU_k can be derived by using (17) and (18) as

$$\begin{aligned} \mathbb{V} \text{ar}(\hat{\mathbf{w}}_k \mathbf{g}_k) &= \mathbb{E} \left[|\hat{\mathbf{w}}_k \mathcal{E}_{G_k}|^2 \right] \\ &= \left(\zeta_{G_k} - \hat{\zeta}_{G_k} \right) \mathbb{E} \left[\|\hat{\mathbf{w}}_k\|^2 \right] \\ &= \left(\zeta_{G_k} - \hat{\zeta}_{G_k} \right) \mathbb{E} \left[\left(\hat{\mathbf{G}}^H \hat{\mathbf{G}} \right)^{-1} \right]_{k,k} \\ &= \frac{\left(\zeta_{G_k} - \hat{\zeta}_{G_k} \right)}{\hat{\zeta}_{G_k} K} \mathbb{E} \left[\text{Tr}(\mathbf{X}^{-1}) \right] \\ &= \frac{\left(\zeta_{G_k} - \hat{\zeta}_{G_k} \right)}{\hat{\zeta}_{G_k} (M - K)}, \end{aligned} \quad (19)$$

where \mathbf{X} is a $K \times K$ central Wishart matrix with N_P degrees of freedom and covariance matrix \mathbf{I}_K , where $\mathbb{E}[\text{Tr}(\mathbf{X}^{-1})] = K/(M - K)$ [42].

¹ZF-type receiver filter performs better than matched-filter detector in terms of nulling the jamming signal [26] and inter-pair interference mitigation [39].

The next term of the inter-user interference $UI_{kk'}$ can be computed from (17), $\hat{\mathbf{w}}_k \mathbf{g}_{k'} = \hat{\mathbf{w}}_k \mathcal{E}_{G_{k'}}$ for $k' \neq k$. Since $\hat{\mathbf{w}}_k$ and $\mathcal{E}_{G_{k'}}$ are uncorrelated, then it can be shown that

$$\begin{aligned} \mathbb{E} \left[|\hat{\mathbf{w}}_k \mathbf{g}_{k'}|^2 \right] &= \left(\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}} \right) \mathbb{E} \left[\left(\hat{\mathbf{G}}^H \hat{\mathbf{G}} \right)^{-1} \right]_{k,k} \\ &= \frac{\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}}{\hat{\zeta}_{G_k} (M - K)}. \end{aligned} \quad (20)$$

Similarly, the noise term obtains as

$$\sigma_n^2 \mathbb{E} \left[\|\hat{\mathbf{w}}_k\|^2 \right] = \frac{\sigma_n^2}{\hat{\zeta}_{G_k} (M - K)}. \quad (21)$$

Then, by substituting (18), (19), (20), and (21) into (15), the achievable rate of the k -th at the base-station can be tightly lower bounded as given below:

$$\bar{R}_U = \frac{(1 - \alpha)T}{T_C} \sum_{k=1}^K \log_2 \left(1 + \frac{P_{d_k} (M - K) \hat{\zeta}_{G_k}}{\sum_{k'=1}^K P_{d_{k'}} (\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}) + \sigma_n^2} \right). \quad (22)$$

B. Uplink Sum Rate for Large Number of Antennas

The asymptotic properties of massive MIMO is utilized in this subsection to obtain a closed-form expression of the asymptotic uplink sum rate. Namely, the number of antennas at the base-station grows unbounded with respect to the number of served user nodes, i.e., the number of users (K) is kept at arbitrary finite value with respect to M . Having been inspired by the power scaling laws of massive MIMO [43], the transmit power at the user nodes can be scaled inversely proportional to the number of antennas at the base-station as $P_d = E_d/M$, where E_d is fixed. In this context, by letting $M \rightarrow \infty$ in (22) and by invoking (9), the SINR of the k -th user node within the asymptotic base-station antenna regime can be derived as

$$\tilde{\gamma}_k^\infty = \frac{\alpha \hat{\zeta}_{G_k}}{(1 - \alpha) \sigma_n^2} \Psi \left(\left\| \mathbf{h}_k \mathbf{P}_E^{1/2} \right\|^2 \right) \quad (23)$$

Then, the obtained asymptotic SINR in (23) can be rewritten as $\tilde{\gamma}_k^\infty = \mathcal{A}_k \Psi(Z)$, where $\mathcal{A}_k = \alpha \hat{\zeta}_{G_k} / ((1 - \alpha) \sigma_n^2)$ and $Z = \|\mathbf{h}_k \mathbf{P}_E^{1/2}\|^2 = \sum_{j=1}^N Z_j$ 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

$$f_{Z_j}(x) = \exp \left(\frac{-x}{\beta_{H_j} P_{E_j}} \right) / (\beta_{H_j} P_{E_j}), \quad x \geq 0. \quad (24)$$

However, when all Z_j s are independent but not identically distributed (i.n.i.d.) with distinct average powers, then the PDF of Z is given by [44]

$$f_Z(z) = \sum_{j=1}^N \frac{\Omega_j}{\beta_{H_j} P_{E_j}} \exp \left(\frac{-z}{\beta_{H_j} P_{E_j}} \right), \quad z \geq 0. \quad (25)$$

where

$$\Omega_j = \prod_{i=1, i \neq j}^N \frac{\beta_{H_j} P_{E_j}}{\beta_{H_j} P_{E_j} - \beta_{H_i} P_{E_i}}. \quad (26)$$

Thus, the average sum rate can be written as

$$\bar{R}_U^\infty = (1 - \alpha) \sum_{k=1}^K \int_0^\infty \log_2(1 + \mathcal{A}_k \Psi(z)) f_Z(z) dz. \quad (27)$$

However, the above expression is mathematically intractable due to the non-linearity of energy harvesting model. To tackle this issue while keeping the analysis tractable, we consider a practical non-linear energy harvesting model in [45], [46], named as constant-linear-constant (CLC), that takes into account both limited sensitivity and saturation of RF energy harvesting. The harvested power in CLC model is expressed as a function of the incident power ρ as given below

$$P_{CLC}(\rho) = \begin{cases} 0, & \rho \in [0, P_{in}^{\text{sen}}], \\ \eta_C (\rho - P_{in}^{\text{sen}}), & \rho \in [P_{in}^{\text{sen}}, P_{in}^{\text{sat}}], \\ \eta_C (P_{in}^{\text{sat}} - P_{in}^{\text{sen}}), & \rho \in [P_{in}^{\text{sat}}, \infty], \end{cases} \quad (28)$$

where constant $\eta_C \in [0, 1)$. P_{in}^{sen} is the sensitivity of the RF harvester, which is the minimum power required to start harvesting, and P_{in}^{sat} accounts for the saturation power threshold, i.e., the harvested power is constant when the input power is greater than P_{in}^{sat} . Thereby, the integral in (27) can be solved using [47, Eq. (4.337.2)], and then, the achievable sum rate can be derived as follows.

$$\bar{R}_U^\infty = \frac{(1 - \alpha)}{\ln(2)} \sum_{k=1}^K \sum_{j=1}^N \tilde{B}_{jk} \left(\prod_{i=1, i \neq j}^N \frac{\beta_{H_j} P_{E_j}}{\beta_{H_j} P_{E_j} - \beta_{H_i} P_{E_i}} \right), \quad (29)$$

where

$$\tilde{B}_{jk} = \begin{cases} 0, & Z \in [0, P_{in}^{\text{sen}}], \\ -\exp \left(\frac{-P_{in}^{\text{sen}}}{\beta_{H_j} P_{E_j}} \right) \exp \left(\frac{1}{\eta_C \mathcal{A}_k \beta_{H_j} P_{E_j}} \right) \times \\ \text{Ei} \left(\frac{-1}{\eta_C \mathcal{A}_k \beta_{H_j} P_{E_j}} \right), & Z \in [P_{in}^{\text{sen}}, P_{in}^{\text{sat}}], \\ \ln(1 + \mathcal{A}_k \eta_C (P_{in}^{\text{sat}} - P_{in}^{\text{sen}})), & Z \in [P_{in}^{\text{sat}}, \infty], \end{cases}$$

where $\text{Ei}(\cdot)$ is the exponential integral function [47].

Remark 1: The uplink sum rate expressions are both monotonically increasing functions with the number of active jammers (N) when the incident jamming power is between the sensitivity and saturation thresholds of the RF harvester. Thus, massive MIMO systems can take advantage of the jamming attacks for boosting the achievable rate, while evidently maintaining the secrecy performance through other efficient secure transmission techniques.

C. Optimization of Time-Switching Factor

In a time-switching energy harvesting protocol, energy harvesting and data transmissions occur sequentially in two orthogonal time-slots αT and $(1 - \alpha)T$, respectively. Therefore, determining the optimal allocation of time for each phase, i.e., the optimal time-switching factor (α), has a significant impact on the system performance. To address this, we formulate two optimization problems in this subsection to achieve α optimality based on user requirements and operating conditions. The first optimization problem maximizes the achievable sum rate, while the second optimization problem ensures fairness among users by maximizing the minimum data rate.

1) *Sum Rate Maximization*: Sum rate is an important indicator for system performance and it is of great interest to massive MIMO systems in order to provide good service under favorable propagation [48]. Thus, the asymptotic expression of the achievable uplink sum rate in (23) with the CLC energy harvesting model in (28) can be utilized for the optimization problem of finding the optimal time switching factor (α) as detailed below

$$\begin{aligned}\alpha^* &= \max_{0 \leq \alpha \leq 1} \bar{R}_U^\infty \\ &= \max_{0 \leq \alpha \leq 1} (1 - \alpha) \sum_{k=1}^K \log_2(1 + \bar{\gamma}_k^\infty) \\ &= \max_{0 \leq \alpha \leq 1} (1 - \alpha) \sum_{k=1}^K \log_2 \left(1 + \frac{\alpha \hat{\zeta}_{G_k}}{(1 - \alpha) \sigma_n^2} P_{CLC} \left(\left\| \mathbf{h}_k \mathbf{P}_E^{1/2} \right\|^2 \right) \right)\end{aligned}\quad (30)$$

The partial derivative of \bar{R}_U^∞ with respect to α can be derived as

$$\frac{\partial \bar{R}_U^\infty}{\partial \alpha} = \sum_{k=1}^K \frac{\nu_k}{1 - \alpha(1 - \nu_k)} - \sum_{k=1}^K \ln \left(1 + \frac{\nu_k \alpha}{1 - \alpha} \right), \quad (31)$$

where ν_k is given by

$$\nu_k = \frac{\hat{\zeta}_{G_k}}{\sigma_n^2} \sum_{k=1}^K P_{CLC} \left(\left\| \mathbf{h}_k \mathbf{P}_E^{1/2} \right\|^2 \right). \quad (32)$$

By letting $\partial \bar{R}_U^\infty / \partial \alpha = 0$, it can be shown that

$$\sum_{k=1}^K \frac{\nu_k}{1 - \alpha(1 - \nu_k)} = \sum_{k=1}^K \ln \left(1 + \frac{\nu_k \alpha}{1 - \alpha} \right), \quad (33)$$

Next, by exploiting the fact that the achievable sum rate maximizes when the achievable rates of individual user nodes are maximized, (33) can be simplified as

$$\exp \left(\frac{\nu_k}{1 - \alpha(1 - \nu_k)} \right) = \frac{1 - \alpha(1 - \nu_k)}{1 - \alpha}, \quad (34)$$

$$\left(\frac{(1 - \alpha)(\nu_k - 1)}{1 - \alpha(1 - \nu_k)} \right) \exp \left(\frac{(1 - \alpha)(\nu_k - 1)}{1 - \alpha(1 - \nu_k)} \right) = \left(\frac{\nu_k - 1}{e} \right). \quad (35)$$

where $e = \exp(1)$.

Next, by using the fact that the solution for $f(x)\exp(f(x)) = y$ is $f(x) = \mathbb{W}(y)$, where $\mathbb{W}(\cdot)$ is the Lambert-W function [49], and hence, (35) can be re-written as:

$$\mathbb{W} \left(\frac{\nu_k - 1}{e} \right) = \frac{(1 - \alpha)(\nu_k - 1)}{1 - \alpha(1 - \nu_k)}. \quad (36)$$

By using (36), the optimal α that maximizes the achievable uplink sum rate can be derived as follows:

$$\alpha^* = \frac{\nu_k - 1 - \mathbb{W} \left(\frac{\nu_k - 1}{e} \right)}{(\nu_k - 1) \left(\mathbb{W} \left(\frac{\nu_k - 1}{e} \right) + 1 \right)}. \quad (37)$$

The second partial derivative of the achievable rate for the k -th user node with respect to α can be derived as

$$\frac{\partial^2 [\bar{R}_U^\infty]_k}{\partial \alpha^2} = \frac{-\nu_k^2}{(1 - \alpha)(\alpha \nu_k - \alpha + 1)^2} < 0 \quad (38)$$

By considering the fact of $\alpha \in [0, 1]$, it can be concluded that $\partial^2 [\bar{R}_U^\infty]_k / \partial \alpha^2 < 0$ for all α . Therefore, the optimal α derived in (37) indeed maximizes the achievable sum rate.

2) *Max-Min Optimization*: The performance optimization while guaranteeing user-fairness in terms of the harvested energy and achievable uplink rate of the user nodes has a significant impact in such compelling scenario in order to fully exploit the available resources. Therefore, we will show that the time-switching factor can be optimized based on the maximum fairness criterion, a max-min optimization problem is 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

$$\underset{\alpha \forall k}{\text{maximize}} \quad \bar{\gamma}_k \quad (39a)$$

$$\text{subject to} \quad \bar{\gamma}_k \Delta_k \geq P_{d_k} (M - K) \hat{\zeta}_{G_k}, \quad \forall k, \quad (39b)$$

$$0 \leq \alpha \leq 1, \quad \forall k, \quad (39c)$$

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 constraints 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^* .

Remark 2: 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 obtain optimal levels of harvested energy and data rate.

D. Rate-Energy Trade-Off

In time-switching protocol, the energy harvesting and data transfers carry out over two sequential time-slots. In details, 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 . Thereby, the rate-energy trade-off can be obtained by first solving for α in (6) and then by substituting the result into (22) as elaborated below

$$\begin{aligned}\bar{R}_U^* &\approx \sum_{k=1}^K \left(\frac{T}{T_C} - \frac{\bar{E}_h}{\left(T_C \sum_{n=1}^N \Psi_{EH_k} (P_{E_n} \beta_{H_{kn}}) \right)} \right) \\ &\times \log_2 \left(1 + \frac{\theta_{d_k} (M - K) \hat{\zeta}_{G_k}}{\sum_{k'=1}^K \theta_{d_{k'}} (\zeta_{G_{k'}} - \hat{\zeta}_{G_{k'}}) + \sigma_n^2} \right)\end{aligned}\quad (40)$$

where θ_{d_k} is defined as

$$\theta_{d_k} = \frac{\bar{E}_h \sum_{n=1}^N \Psi_{EH_k} (P_{E_n} \beta_{H_{kn}})}{T \sum_{n=1}^N \Psi_{EH_k} (P_{E_n} \beta_{H_{kn}}) - \bar{E}_h}. \quad (41)$$

Remark 3: The energy-rate trade-off expression in (40) is optimal due to the max-min user-fairness when setting the harvested energy targets of each user to a common value \bar{E}_h . Thereby, the max-min optimal time-switching factor corresponding to any system operating point can be attained by applying this optimal energy-rate trade-off.

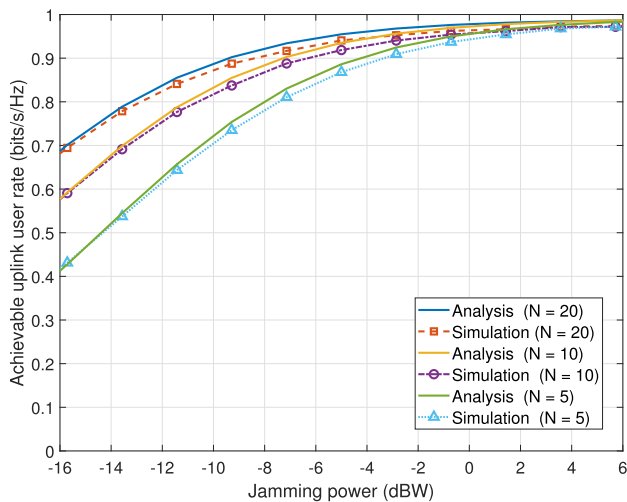


Fig. 3. Achievable uplink user rate versus jamming power when $K = 5$, $M = 20$, $\alpha = 0.5$, and different number of active attackers (N).

IV. NUMERICAL RESULTS

In this section, we evaluate the performance of the proposed energy harvesting scheme. To capture the effects of practical transmission impairments, the channel path-loss is modeled as $[PL]_{\text{dB}} = PL_0 + 10v \log(d)$, where $PL_0 = 20 \log(4\pi d_0/\lambda)$ is the path-loss at the reference distance d_0 , d is the distance between the transmitter and receiver, and v is the path-loss exponent. Unless otherwise specified, the simulation parameters are set to $v = 2.3$, $d_0 = 1$ m, $d_G = 100 - 300$ m, $d_H = 100 - 500$ m, $\sigma_n^2 = 0$ dBW, and $\mathcal{P}_P = 0$ dBW. The coherence time is set to $T_C = 1$ ms having 196 symbols, pilot length is $T_p = K$ [39].

The considered energy harvesting models in our work have been thoroughly studied and evaluated in [45], [46], [50] to point out the discrepancies between their properties in harvesting RF energy. The findings in these research works have verified that the linear energy harvesting model miscalculates the harvested energy by neglecting the non-linearity of practical energy harvesting rectenna circuits. Therefore, the practical non-linear characteristics of the RF energy harvesting circuit have been taken into consideration in this paper, which minimizes the possibility of performance mismatching with practical systems in this aspect.

In Fig. 3, the average achievable user data rate at the base-station 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 (22), and are compared to the Monte-Carlo simulations of the uplink rate expression in (14) while employing the non-linear harvesting model in (8). Obviously, the achievable rate gradually increases when the jammers transmit higher power levels because the more jamming power, the greater energy will be harvested by the user nodes until a saturation point. This is an explicit consequence of the saturation effect of the non-linear energy harvesting model. Moreover, increasing the number of jamming attacks in the proximity of the served area contributes to harvest more energy and eventually achieves higher data rate. Our analysis is compared to the

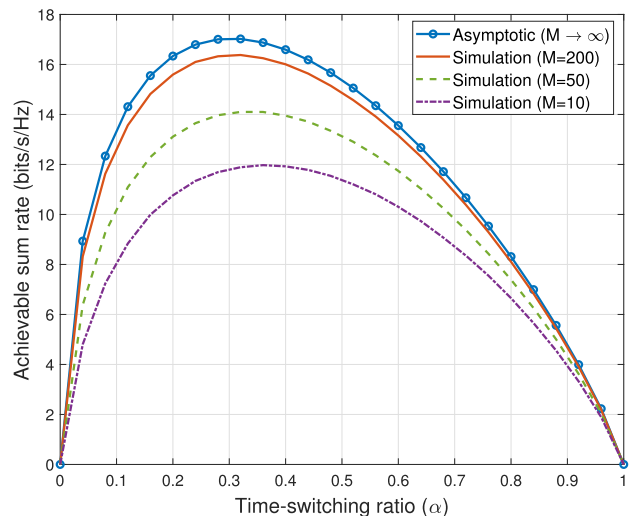


Fig. 4. Achievable uplink sum rate versus time-switching factor (α) for different number of base-station antennas (M) when $K = 5$, $N = 5$, and $P_E = -1$ dBW.

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.

The asymptotic uplink sum rate is plotted as a function of the time switching factor (α) in Fig. 4 for the infinite antenna regime at the base-station, i.e., with progressively increasing the number of antennas M . The asymptotic sum rate curves are plotted by using (29) and compared to the Monte-Carlo simulations in order for validating the accuracy of our analysis. Fig. 4 reveals that the theoretical/asymptotic sum rate limits in (29) can be attained when the number of base-station antennas grows large. Additionally, we notice the following essential design insights. The sum rate approaches its maximum at the optimal α and then decreases thereafter. When α is small, the harvested energy by the user nodes is not adequate to achieve high sum rate. Nonetheless, a too large α value leads to more harvested energy but less residual time for the data transmission, which degrades the sum data rate performance. Thus, there exists a fundamental trade-off between harvested energy and uplink data rate, which will be further explored in the forthcoming evaluation results.

The proposed optimization problem for maximizing the uplink sum rate with respect to the time-switching factor (α) is investigated in Fig. 5 for different values of the jamming powers. Specifically, the achievable sum rate is plotted against α where the optimal α^* is calculated by closed-form solution of (37). Fig. 5 shows that the sum rate versus α is a convex function. Clearly, the achievable rate increases with α when $\alpha \leq \alpha^*$, and then decreases if $\alpha > \alpha^*$. Accordingly, the maximum achievable rate is attained at α^* , which is consistent with the obtained analytical results for maximizing the sum rate in Section III-C1. Further, the optimal α^* itself decreases when there is more jamming power to harvest, which eventually spares more time for data transmission and increases the sum data rate. This observation verifies that the proposed jamming energy harvesting scheme is beneficial in boosting the performance of massive MIMO systems.

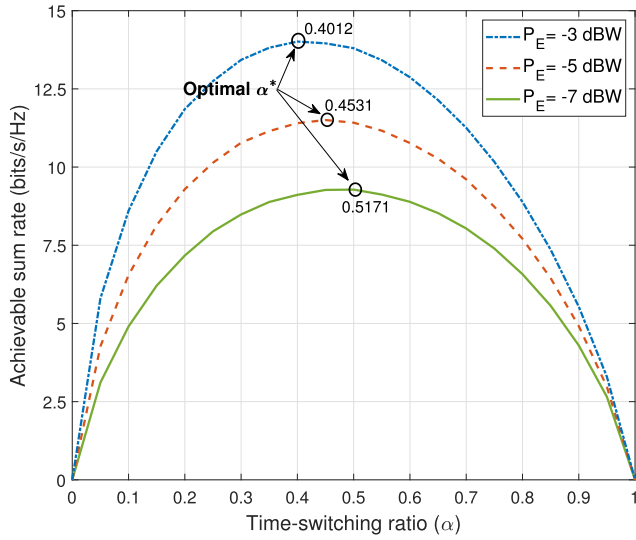


Fig. 5. Optimization of time-switching factor (α) for maximizing the achievable uplink sum rate with considering different levels of jamming power.

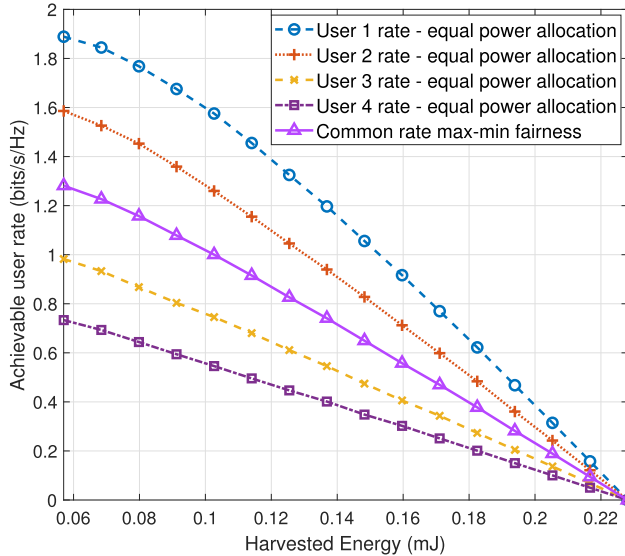


Fig. 6. A comparison of the achievable uplink data rate and the harvested energy between the uniform and max-min user-fairness power allocation policies.

The proposed max-min fairness-based problem for optimizing α to achieve a common data rate among the served users is evaluated in Fig. 6. For the comparison purposes, the achievable user rates is plotted against the harvested energy, when α increases from 0.2 to 1, for (i) the equal power allocation scheme and (ii) optimal power allocation with max-min fairness policy. The considered users are spatially distributed as $\mathbf{d}_{\mathbf{G}} = [150, 180, 220, 250]$ m. The power allocation coefficients for the optimal power allocation are computed by solving the geometric program in (39a)-(39c) using MATLAB CVX. The individual user data rate with the equal power control is mainly affected by the channel conditions or the spatial location of the distributed users. For instance, when the equal power allocation policy is employed, the nearest user (User 1) obtains the best data rate trade, while the farthest user

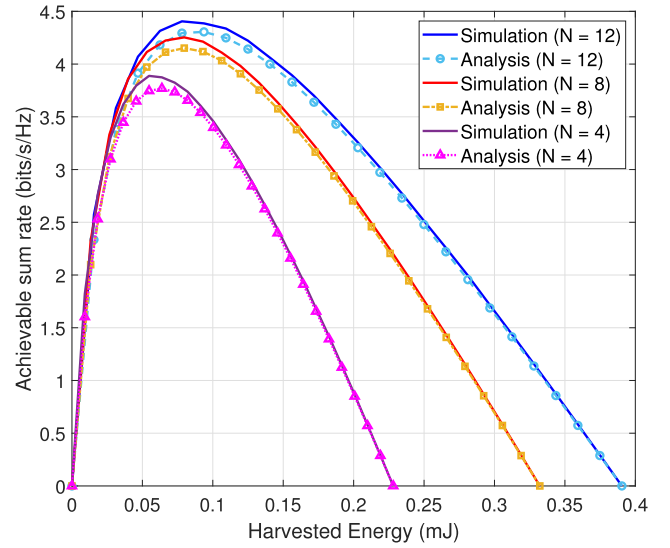


Fig. 7. The rate-energy trade-off. A comparison between uplink sum rate versus the harvested energy for $K = 4$, $M = 15$.

(User 4) experiences the lowest data rate. Clearly, the equal power allocation policy does not guarantee fairness in terms of user data rate. Nevertheless, the proposed max-min fairness power control provides a common achievable rate for every user regardless of its spatial location. Thereby, the proposed max-min power allocation jointly guarantees user-fairness in terms of both the achievable rate and harvested energy. Thus, the validity of the analytical results is corroborated.

The analysis of the rate-energy trade-off in Section III-D is investigated in Fig. 7. Specifically, the achievable uplink sum rate with respect to the harvested energy at the user nodes is plotted for different number of jammers (N) in the finite base-station antenna regime. We used the derived rate-energy trade-off expression in (40) to plot the analytical curves. Fig. 7 clearly reveals that the uplink achievable rate becomes a maximum when the harvested energy approaches the common rate-energy trade-offs. However, the achievable uplink data rate becomes infinitesimal when α approaches one, whereas the harvested energy becomes a maximum value due to the fact that the users harvest energy for the entire transmission frame. Further, as mentioned earlier 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 (40).

V. CONCLUSION

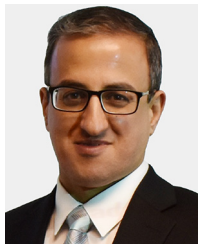
In this paper, we proposed an energy harvesting scheme to exploit the jamming transmissions of the active attackers in massive MIMO systems. Specifically, a wireless-powered multi-user massive MIMO system has been considered where user nodes harvest energy from the jamming signals and utilize it for information transmission. The feasibility of proposed concept has been investigated by system performance analysis for a training-based massive MIMO involves imperfectly

estimated CSI at the base-station and employing the time-switching protocol. In particular, the harvested energy, SINR, and sum rate expressions have been derived for finitely many base-station antennas, where a tight sum rate expression is obtained in closed-form. The asymptotic performance metrics are also provided when the numbers of base-station antennas grow large. In addition, two optimization problems are formulated and solved to achieve optimal time switching factor based on maximizing the uplink sum rate and jointly ensuring user-fairness in terms of energy and rate. Furthermore, the fundamental trade-off between the harvested energy and achievable sum rate in time-switching protocol is quantified in closed-form expression. The conducted analyses in this work have shown the benefits of leveraging the transmitted signals from multiple i.n.i.d. jammers for energy harvesting in multi-user massive MIMO communication systems. Finally, the performance metrics have been analytically and numerically evaluated over various antenna configurations and setups where the obtained results have validated the feasibility of the proposed energy harvesting scheme in boosting the massive MIMO uplink performance.

REFERENCES

- [1] H. Al-Hraishawi, S. Chatzinotas, and B. E. Ottersten, "Exploiting jamming attacks for energy harvesting in massive MIMO systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Montreal, QC, Canada, Jun. 2021, pp. 1–6.
- [2] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun. Mag.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.
- [3] H. J. Visser and R. J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: Principles and requirements," *Proc. IEEE*, vol. 101, no. 6, pp. 1410–1423, Jun. 2013.
- [4] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.
- [5] M.-T. Chiu, C.-Y. Chiu, C. Ng, L.-O. Wong, S. Shen, and R. Murch, "An ambient RF powered wireless sensor system," *IEEE Open J. Antennas Propag.*, vol. 3, pp. 1382–1393, 2022.
- [6] M. Wang, Y. Lin, Q. Tian, and G. Si, "Transfer learning promotes 6G wireless communications: Recent advances and future challenges," *IEEE Trans. Rel.*, vol. 70, no. 2, pp. 790–807, Jun. 2021.
- [7] 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, Apr. 2015.
- [8] E. Goudeli, C. Psomas, and I. Krikidis, "A detection scheme for integrated SWIPT receivers with rectenna arrays," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 1, pp. 145–157, Mar. 2023.
- [9] L. Chen, F. R. Yu, H. Ji, B. Rong, X. Li, and V. C. M. Leung, "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.
- [10] K. Huang and V. K. N. Lau, "Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 902–912, Feb. 2014.
- [11] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.
- [12] H. Al-Hraishawi and G. A. A. Baduge, "Wireless energy harvesting in cognitive massive MIMO systems with underlay spectrum sharing," vol. 6, no. 1, pp. 134–137, Feb. 2017.
- [13] H. Wang, W. Wang, X. Chen, and Z. Zhang, "Wireless information and energy transfer in interference aware massive MIMO systems," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Austin, TX, USA, Dec. 2014, pp. 2556–2561.
- [14] D. Kudathanthirige, R. Shrestha, and G. A. A. Baduge, "Wireless information and power transfer in relay-assisted downlink massive MIMO," *IEEE Trans. Green Commun. Netw.*, vol. 3, no. 3, pp. 789–805, Sep. 2019.
- [15] B. Li, Y. Dai, Z. Dong, E. Panayirci, H. Jiang, and H. Jiang, "Energy-efficient resources allocation with millimeter-wave massive MIMO in ultra dense HetNets by SWIPT and CoMP," *IEEE Trans. Wireless Commun.*, vol. 20, no. 7, pp. 4435–4451, Jul. 2021.
- [16] V. Khodamoradi, A. Sali, O. Messadi, A. Khalili, and B. B. M. Ali, "Energy-efficient massive MIMO SWIPT-enabled systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 5111–5127, May 2022.
- [17] H. Al-Hraishawi, G. A. A. Baduge, H. Q. Ngo, and E. G. Larsson, "Multi-cell massive MIMO uplink with underlay spectrum sharing," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 1, pp. 119–137, Mar. 2019.
- [18] 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, Jun. 2018.
- [19] H. Al-Hraishawi, G. Amarasuriya, and R. F. Schaefer, "Secure communication in underlay cognitive massive MIMO systems with pilot contamination," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Singapore, Dec. 2017, pp. 1–7.
- [20] M. Vanhoef and F. Piessens, "Advanced Wi-Fi attacks using commodity hardware," in *Proc. 30th Annu. Comput. Security Appl. Conf. (ACSAC)*, New Orleans, LA, USA, Dec. 2014, pp. 256–265.
- [21] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.
- [22] 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.
- [23] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Philadelphia, PA, USA, Sep. 2015, pp. 272–280.
- [24] T. T. Nguyen and K.-K. Nguyen, "Anti-jamming in cell free mMIMO systems," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Madrid, Spain, Dec. 2021, pp. 1–6.
- [25] Z. Shen, K. Xu, and X. Xia, "Beam-domain anti-jamming transmission for downlink massive MIMO systems: A Stackelberg game perspective," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2727–2742, 2021.
- [26] 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.
- [27] W. Xu, B. Li, L. Tao, and W. Xiang, "Artificial noise assisted secure transmission for uplink of massive MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6750–6762, Jul. 2021.
- [28] 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.
- [29] 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, Jun. 2019.
- [30] 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, Apr. 2020.
- [31] J. Xu, W. Xu, D. W. K. Ng, and A. L. Swindlehurst, "Secure communication for spatially sparse millimeter-wave massive MIMO channels via hybrid precoding," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 887–901, Feb. 2020.
- [32] Z. Fang, T. Song, and T. Li, "Energy harvesting for two-way OFDM communications under hostile jamming," *IEEE Signal Process. Lett.*, vol. 22, no. 4, pp. 413–416, Apr. 2015.
- [33] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2611–2626, Nov. 2017.
- [34] J. Guo, N. Zhao, F. R. Yu, X. Liu, and V. C. M. Leung, "Exploiting adversarial jamming signals for energy harvesting in interference networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1267–1280, Feb. 2017.
- [35] G. Rezgui, E. V. Belmega, and A. Chorti, "Mitigating jamming attacks using energy harvesting," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 297–300, Feb. 2019.
- [36] L. Xiao, Y. Li, C. Dai, H. Dai, and H. V. Poor, "Reinforcement learning-based NOMA power allocation in the presence of smart jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3377–3389, Apr. 2017.
- [37] A. Sheikhi, S. M. Razavizadeh, and I. Lee, "A comparison of TDD and FDD massive MIMO systems against smart jamming," *IEEE Access*, vol. 8, pp. 72068–72077, Apr. 2020.

- [38] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.
- [39] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2016.
- [40] S. M. Kay, *Fundamentals of Statistical Signal Processing: Practical: Algorithm Development*. Upper Saddle River, NJ, USA: Prentice-Hall, Apr. 1993.
- [41] E. Boshkovska, D. W. K. Ng, N. Zlatanov, and R. Schober, "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2082–2085, Dec. 2015.
- [42] A. M. Tulino and S. Verdú, "Random matrix theory and wireless communications," *Found. Trends Commun. Inf. Theory*, vol. 1, no. 1, pp. 1–128, Jun. 2004.
- [43] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.
- [44] J. Proakis, *Digital Communications*, 4th ed. New York, NY, USA: McGraw-Hill, Aug. 2001.
- [45] P. N. Alevizos and A. Bletsas, "Sensitive and nonlinear far-field RF energy harvesting in wireless communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3670–3685, Jun. 2018.
- [46] A. Hakimi, M. Mohammadi, Z. Mobini, and Z. Ding, "Full-duplex non-orthogonal multiple access cooperative spectrum-sharing networks with non-linear energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 10925–10936, Oct. 2020.
- [47] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Cambridge, MA, USA: Academic, 2007.
- [48] H. Yang and T. L. Marzetta, "Massive MIMO with max–min power control in line-of-sight propagation environment," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4685–4693, Nov. 2017.
- [49] R. M. Corless, G. H. Gonne, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, "On the lambert W function," *Adv. Comput. Math.*, vol. 5, no. 1, pp. 329–359, Dec. 1996.
- [50] S. A. A. Kazmi and S. Coleri, "Optimization of full-duplex relaying system with non-linear energy harvester," *IEEE Access*, vol. 8, pp. 201566–201576, 2020.



Hayder Al-Hraishawi (Senior Member, IEEE) received the Ph.D. degree in engineering from the Department of Electrical and Computer Engineering, Southern Illinois University Carbondale, USA, in 2017. He is currently a Research Scientist with the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg. He is an experienced engineering professional with over five years of industrial and leadership experience gained from holding various positions at reputable telecom companies, such as Motorola Solutions, Huawei Technologies, and Nokia Networks. His research interests span the broad areas of terrestrial and non-terrestrial communications networks and signal processing, including spectrum-sharing and resource allocation techniques for massive MIMO systems, reconfigurable intelligent surfaces, and satellite communication systems. He has been a member (Associate Editor) in the editorial board of IEEE ACCESS since 2019. He was an Exemplary Reviewer for the IEEE TRANSACTION ON COMMUNICATIONS in 2022. He has served as a Technical Program Committee Member for several IEEE conferences, including ICC and GLOBECOM.



Osamah A. Abdullah received the Ph.D. degree in electrical and computer engineering from Western Michigan University, USA, in 2016. He is currently an Assistant Professor with the Ministry of Higher Education and Scientific Research, Iraq. He has a strong academic background, having previously taught at Al-Mamoun University College and served as the Department Head with teaching responsibilities with Madenat Alelem University College, Baghdad. In addition to his academic experience, he has gained valuable industry knowledge through his

role as a planning and an Optimization Engineer with Huawei Technologies, where he worked on the Asiacell Cellular Network Project, Iraq. His research interests encompass various areas, including wireless communication systems, machine learning algorithms, signal processing, channel modeling, brainwave signal detection, and peer-to-peer/ad hoc networking with a particular focus on applications related to group localization, tracking, and monitoring.



Symeon Chatzinotas (Fellow, IEEE) received the M.Eng. degree in telecommunications from the Aristotle University of Thessaloniki, Greece, in 2003, and the M.Sc. and Ph.D. degrees in electronic engineering from the University of Surrey, U.K., 2006 and 2009, respectively. He is currently a Full Professor/Chief Scientist I and the Head of the Research Group SIGCOM in the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg. In the past, he has lectured as a Visiting Professor with the University of Parma, Italy, and contributed in numerous research and development projects for the Institute of Informatics and Telecommunications, National Center for Scientific Research "Demokritos," the Institute of Telematics and Informatics, Center of Research and Technology Hellas and Mobile Communications Research Group, Center of Communication Systems Research, University of Surrey. He has authored more than 700 technical papers in refereed international journals, conferences and scientific books. He has received numerous awards and recognitions, including the IEEE Fellowship and an IEEE Distinguished Contributions Award. He is currently in the editorial board of the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE OPEN JOURNAL OF VEHICULAR TECHNOLOGY, and the *International Journal of Satellite Communications and Networking*.



Björn Ottersten (Fellow, IEEE) received the M.S. degree in electrical engineering and applied physics from Linköping University, Linköping, Sweden, in 1986, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, USA, in 1990. He has held research positions with the Department of Electrical Engineering, Linköping University, the Information Systems Laboratory, Stanford University, the Katholieke Universiteit Leuven, Leuven, Belgium, and the University of Luxembourg, Luxembourg. From 1996 to 1997, he

was the Director of Research with ArrayComm, Inc., a start-up in San Jose, CA, USA, based on his patented technology. In 1991, he was appointed as a Professor of Signal Processing with the Royal Institute of Technology, Stockholm, Sweden, where he has been the Head of the Department for Signals, Sensors, and Systems, and the Dean of the School of Electrical Engineering. He is currently the Director for the Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg. He is a recipient of the IEEE Signal Processing Society Technical Achievement Award, the EURASIP Group Technical Achievement Award, and the European Research Council Advanced Research Grant Twice. He has coauthored journal papers that received the IEEE Signal Processing Society Best Paper Award in 1993, 2001, 2006, 2013, and 2019, and nine IEEE Conference Papers Best Paper Awards. He has been a Board Member of IEEE Signal Processing Society and the Swedish Research Council and currently serves of the boards of EURASIP and the Swedish Foundation for Strategic Research. He has served as an Editor in Chief of EURASIP Signal Processing, and acted on the editorial boards of IEEE TRANSACTIONS ON SIGNAL PROCESSING, *IEEE Signal Processing Magazine*, IEEE OPEN JOURNAL FOR SIGNAL PROCESSING, *EURASIP Journal of Advances in Signal Processing*, and *Foundations and Trends in Signal Processing*. He is a Fellow of EURASIP.