Secrecy Rate Beamforming for Multicell Networks With Information and Energy Harvesting


Published in:
IEEE Transactions on Signal Processing

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person’s rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.
Secrecy Rate Beamforming for Multi-cell Networks with Information and Energy Harvesting

Ali Arshad Nasir, Hoang Duong Tuan, Trung Q. Duong, and H. Vincent Poor

Abstract—Considering a multicell network for secure wireless information and power transfer, this paper studies the joint design of transmit beamformers at the base stations (BSs) and receive signal splitting ratios at the end users’ equipment (UEs). The primary concern in this work is the network internal security, where there may be a single multi-antenna eavesdropper or there is a risk that any near user may accidentally eavesdrop on the received signal of any far user. The objective is to maximize the minimum secrecy user rate under BS transmit power and UE minimum harvested energy constraints. New path-following algorithms are proposed for computational solutions of these difficult nonconvex optimization problems. Each iteration involves one simple convex quadratic program (QP). Numerical results confirm that the proposed algorithms converge quickly after few iterations having low computational complexity.

Index Terms—Secure communication, secrecy rate, energy harvesting, nonconvex programming, wireless information and power transfer, signal splitting, transmit beamforming.

I. INTRODUCTION

The openness of the wireless medium and the broadcast nature of wireless networks makes them vulnerable to malicious attacks of adversaries [1]–[4]. Adversaries may attempt to launch various attacks to disrupt or eavesdrop upon the normal information flows [5]. The traditional encryption for secure information transfer may be not practical for certain emerging wireless networking paradigms, such as the Internet of Things or ad hoc networks, due to lack of infrastructure or due to low complexity of terminals. Physical layer security (PLS) [6], [7], which explores the ability of the wireless physical layer to provide secrecy in data transmissions is a compelling approach to providing security in such networks [7]–[9]. The secrecy rate in PLS characterizes the ability of users to transmit messages to intended users while keeping the messages confidential from eavesdroppers [7], [10]. Note that registered network users may also play the role of eavesdroppers to decode information intended for other users in the network, which is also related to the concept of internal network security [11].

Recently, dense small-cell deployment has been identified as one of the ‘big pillars’ to support the much needed 1,000× increase in data throughput for the fifth-generation (5G) wireless networks [12]. Moreover, the benefits of coordination among small cells have been very recently reported [13]. In such setup, small-cell users become more prone to being eavesdropped upon due to closer proximity among users. Furthermore, there is a major concern with the energy consumption of such a dense small-cell deployment. Recent advances in wireless power transfer allow the emitted energy in the radio frequency (RF) signals to be harvested and recycled [14]. Wireless power transfer from a BS to its users (UEs) is viable in a dense small-cell environment, because the close BS-UE proximity enables an adequate amount of RF energy to be harvested for practical applications [15].

Recently, transmit beamforming design at the base station (BS) for secrecy rate maximization under BS transmit power constraints has achieved researchers’ considerable attention [16]–[21]. A common approach to such design problems is to formulate them as optimization of the outer products of the beamforming vectors. The rank-one constraints on these outer products are then dropped to translate into rank-dropped programs, which however are still nonconvex due to the presence of the eavesdropper rates in the objective. A simple semi-definite programming (SDP) relaxation for these rank-dropped programs was proposed in [17], while in [19], they were addressed by successive SDP, which involves a substantial number of additional variables. Randomization was used in [17] and [19] to generate feasible beamforming vectors from the found matrix solution of the rank-dropped program. As noted in [22], such randomization is not efficient. However, it should be noted that these rank-dropped programs are examples of d.c. (difference of two convex functions) programming, which can be easily and effectively solved by d.c. iterations [23].

Meanwhile, simultaneous wireless information and power transfer (SWIPT) has been proposed as a promising wireless energy harvesting (EH) technique in energy constrained networks [14], [24]–[26], such as those for which PLS may be most appropriate. Thus, for SWIPT systems, there is an inclusion of receiver energy harvesting constraints in the secrecy rate maximization problem, which is not only non-convex but also conflicting with both information throughput and communication security. Secure beamforming in SWIPT systems is relevant, since not only the active network eavesdroppers, but also the receivers employing energy harvesting, being located close to the BS to enable meaningful EH [20], can potentially eavesdrop upon other users’ information [20], [27].
EH constrained secrecy rate maximization for single-input-single-output (SISO) [11], [28], multiple-input-single-output (MISO) [20], [21], [29]–[31], and multiple-input-multiple-output (MIMO) [32], [33] systems, and single-antenna AF relaying network [34] has been studied. Most of the these works [11], [20], [21], [28], [31]–[33] assume either energy harvesting (EH) functionality or information decoding (ID) functionality at the receiver. To enable simultaneous EH and ID (SWIPT) in practical networks, a receiver must employ power splitting (PS) scheme whereby the received signal from the BS is divided into information and energy streams [30].

Regarding beamforming design, following [17] for secrecy rate maximization, [29]–[31] reformulated EH constrained secrecy rate maximization by optimizing the outer products of beamforming vectors. The rank-one constraints on these outer products were also dropped in [29] and [30] to produce rank-dropped programs. It should be noted that under this reformulation, the addition of EH constraints does not change the nature of the optimization problems. Based on the found matrix solution of the rank-dropped programs, randomization was also used in [29] and [30] to find feasible beamforming vectors. In [31], the eavesdropping rate is delegated to a highly nonlinear determinant constraint in the outer products of the beamforming vectors, which is then relaxed to a convex constraint [31, Proposition 1]. The exact penalty function optimization approach of [22] was used in [31] to handle the rank-one constraints on these outer-products. It is easily seen that by using the exact penalty function optimization approach of [22], the EH constrained secrecy rate maximization is equivalent to d.c. programs in the outer products of beamforming vectors, which again can be solved by d.c. iterations [23].

In this paper, we consider a multicell network, in which a multi-antenna BS in each cell communicates with its respective users (UEs). The UEs are divided into two groups on the basis of their distance from the serving BS. The UEs in the near vicinity of the BS (near UEs) implement SWIPT while far-away UEs (far UEs) conduct information decoding only. We consider two different eavesdropper models. In the first model (Eve Model 1), we assume a single multi-antenna eavesdropper, who tries to decode information for any user equipment (UE). Thus, we aim to jointly optimize transmit beamforming vectors, transmit artificial noise vectors (helps to reduce signal-to-interference-plus-noise-ratio (SINR) at the eavesdropper and increase the harvested energy for near UEs), and receiver PS ratios for near UEs to maximize the worst secrecy rate of all UEs under EH constraints for near UEs and BS transmit power constraints. In our second model (Eve Model 2), we consider a more practical scenario of the network internal security where any user among near UEs may accidentally eavesdrop on the received signal of any user among far UEs. Thus, we aim to maximize the worst secrecy rate of far UEs under minimum SINR and EH constraints for near UE and BS transmit power constraints. We propose path-following optimization algorithms to solve these two EH constrained secrecy rate problems. Avoiding rank-constrained optimization, our algorithms require minimum number of variables, and computationally quite fast as converges in few iterations. We compare the EH constrained secrecy rate performance with the normal rates achieved in the absence of eavesdroppers. Our simulation results show that secrecy rate of our proposed algorithms is close to the achievable normal rates in the absence of eavesdroppers. Furthermore, the secrecy rate of the Eve Model 2 is better than that of the Eve Model 1 due to the presence of multi-antenna eavesdropper in Eve Model 1.

The paper is organized as follows. Section II presents the system model and problem formulation. Section III proposes path-following iterative algorithms for the solutions. Section IV evaluates the performance of our proposed algorithms by numerical examples. Finally, Section V concludes the paper.

Standard notation used in the paper. Bold symbols are used to represent vectors and matrices. \( R^n \) defines the real operator, \( \nabla \) defines the first-order differential operator, \( \text{Trace}(X) \) is the trace of matrix \( X \), and \( \langle x, y \rangle \equiv x^H y \).

II. SYSTEM MODEL AND PROBLEM FORMULATION

Consider a downlink of a dense network consisting of \( K \) small cells with universal frequency reuse. As shown in Fig. 1, the BS of a cell \( k \in K = \{1, \ldots, K\} \) is equipped with \( M > 1 \) antennas and it serves \( N_k \) single-antenna UEs within its cell. By BS \( k \) and UE \( (k, n) \), we mean the BS that serves cell \( k \) and the UE \( n \in N_k = \{1, \ldots, N_k\} \) of the same cell, respectively. The \( N_k \) UEs in cell \( k \) are divided into two groups, i.e., i) \( N_{1,k} \) zone-1 users, which are located nearby their serving BS inside the inner circle, and ii) \( N_{2,k} \) zone-2 users, which are located far from their serving BS in the outer circle, such that, \( N_k = N_{1,k} + N_{2,k} \). By UE \( (k, n_1) \) and UE \( (k, n_2) \), we mean UE \( n_1 \in N_{1,k} = \{1, \ldots, N_{1,k}\} \) in zone-1 and UE \( n_2 \in N_{2,k} = \{N_{1,k} + 1, \ldots, N_k\} \) in zone-2 of cell \( k \), respectively.
Let us denote by $\mathbf{w}_{k,n} \in \mathbb{C}^{M \times 1}$ the beamforming vector by BS $k$ for its UE $(k,n)$. Let $\mathbf{h}_{k,k,n} \in \mathbb{C}^{M \times 1}$ be the flat fading channel vector between BS $k$ and UE $(k,n)$, which includes the effects of large-scale pathloss and small-scale fading, where $k \in \mathcal{K}$. Let us denote by $x_{k,n}$ the information signal to be transmitted by BS $k$ to UE $(k,n)$ with $\mathbb{E}\{|x_{k,n}|^2\} = 1$. The complex baseband signal received by UE $(k,n)$ is then expressed as

$$y_{k,n} = \sum_{k \in \mathcal{K}} \mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n} x_{k,n} + \sum_{k \in \mathcal{K}} \mathbf{h}_{k,k,n}^H \mathbf{v}_k + z_{k,n},$$

where $\mathbf{v}_k$ is the artificial interference signal added by BS $k$ to confuse the eavesdroppers [35], $z_{k,n} \sim \mathcal{CN}(0, \sigma_n^2)$ is the zero-mean circularly symmetric complex Gaussian noise with variance $\sigma_n^2$ at the receiver of UE $(k,n)$. To show the effect of interference at UE $(k,n)$, let us explicitly write (1) as

$$y_{k,n} = \sum_{k \in \mathcal{K}} \mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n} x_{k,n} + \sum_{k \in \mathcal{K}} \mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n} x_{k,n} + \mathbf{h}_{k,k,n}^H \mathbf{v}_k + \sum_{k \in \mathcal{K}} \mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n} x_{k,n} + z_{k,n},$$

The first term in (2) is the intended signal for UE $n$, the second term is the intercell interference from within cell $k$, and the third term is the intercell interference from other cells $\hat{k} \in \mathcal{K} \setminus \{k\}$.

We assume that zone-1 users, being close to their serving BS, implement SWIPT, such that UE $(k,n)$ applies the power splitting (PS) technique to coordinate both information decoding (ID) and energy harvesting (EH). The power splitter divides the received signal into two parts in the proportion of $\alpha_{k,n} : 1 - \alpha_{k,n}$, where $\alpha_{k,n} \in (0,1)$ is termed as the PS ratio for UE $(k,n)$. The first part $\sqrt{\alpha_{k,n}} y_{k,n}$ forms an input to the ID receiver as

$$\sqrt{\alpha_{k,n}} y_{k,n} + z_{k,n} \triangleq \sqrt{\alpha_{k,n}} x_{k,n} + \sum_{k \in \mathcal{K}} \mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n} x_{k,n} + \mathbf{h}_{k,k,n}^H \mathbf{v}_k + z_{k,n},$$

where $z_{k,n} \sim \mathcal{CN}(0, \sigma_n^2)$ is the additional noise introduced by the ID receiver circuitry. The received SINR of UE $(k,n)$ is given by

$$\text{SINR-UE}_{k,n} = f_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) \triangleq \frac{|\mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n}|^2}{\varphi_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n})},$$

where we denote $\mathbf{w} \triangleq [\mathbf{w}_{k,n}]_{k \in \mathcal{K}, n \in \mathcal{N}_k}$, $\mathbf{v} \triangleq [\mathbf{v}_k]_{k \in \mathcal{K}}$, $\alpha \triangleq [\alpha_{k,n}]_{k \in \mathcal{K}, n \in \mathcal{N}_k}$, $\alpha_{k,n} = \begin{cases} \alpha_{k,n}, & n \in \mathcal{N}_1,k, \\ 1, & n \in \mathcal{N}_2,k, \end{cases}$ and $\varphi_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) \triangleq \sum_{n \in \mathcal{N}_k \setminus \{n\}} |\mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n}|^2 + |\mathbf{h}_{k,k,n}^H \mathbf{v}_k|^2 + \sum_{k \in \mathcal{K} \setminus \{k\}} \sum_{n \in \mathcal{N}_k} |\mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n}|^2 + \frac{\sum_{k \in \mathcal{K}} \sum_{n \in \mathcal{N}_k} |\mathbf{h}_{k,k,n}^H \mathbf{v}_k|^2}{\sum_{k \in \mathcal{K}} |\mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n}|^2 + N_0 \sigma_n^2}.$

The second part $\sqrt{1 - \alpha_{k,n}} y_{k,n}$ of the received signal is processed by an EH receiver. The energy harvested at UE $(k,n)$ is given by

$$E_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) \triangleq \zeta_{k,n} (1 - \alpha_{k,n}) \mathbb{E}(\mathbf{w}_{k,n}^H \mathbf{v}_k),$$

where $\mathbb{E}(\mathbf{w}_{k,n}^H \mathbf{v}_k) \triangleq \sum_{k \in \mathcal{K}} \sum_{n \in \mathcal{N}_k} |\mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n}|^2 + \frac{\sum_{k \in \mathcal{K}} \sum_{n \in \mathcal{N}_k} |\mathbf{h}_{k,k,n}^H \mathbf{v}_k|^2}{\sum_{k \in \mathcal{K}} |\mathbf{h}_{k,k,n}^H \mathbf{w}_{k,n}|^2 + N_0 \sigma_n^2}.$

In the following subsections, we consider two different eavesdroppers model and the corresponding problem formulations.

A. Single Active Eavesdropper Model (Eve Model 1)

Following [10], we first consider the scenario in which a single active eavesdropper $k$ with $N_{ev}$ antennas is registered in the cell $k$ as a subscribed user and exchanges signalling messages with BS $k$. The only objective of this malicious user is to decode information for any UE $(k,n)$. Thus the signal for any UE $(k,n)$ observed at the eavesdropper (EV) $k$ in cell $k$, $\mathbf{y}_k \in \mathcal{C}^{N_{ev} \times 1}$, is given by

$$\mathbf{y}_k = \sum_{k \in \mathcal{K}} \mathbf{H}_{k,k}^H \sum_{n \in \mathcal{N}_k} (\mathbf{w}_{k,n} x_{k,n} + \mathbf{v}_k) + z_k^e,$$

where $\mathbf{H}_{k,k}$ of size $M \times N_{ev}$ is the corresponding wiretap channel between BS $k$ and EV $k$ and $z_k^e \in \mathcal{C}^{N_{ev} \times 1}$ is the zero-mean Gaussian noise with variance $\sigma^2_e$ at each receive antenna. As the EV is registered it is natural to assume that the wiretap channel state information $\mathbf{H}_{k,k}$ is known [10]. Therefore, the received SINR corresponding to the signal intended for the UE $(k,n)$ at the EV $k$ is given by

$$\text{SINR-EV}_{k,n} \triangleq \frac{||\mathbf{H}_{k,k}^H \mathbf{w}_{k,n}||^2}{q_{k,n}(\mathbf{w}, \mathbf{v})}.$$
The achievable secrecy rate at UE \((k, n)\) in nat/sec/Hz is thus given by [36]

\[
f_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) = \ln(1 + \text{SINR-UE}_{k,n}) - \ln(1 + \text{SINR-EV}_{k,n})
\]

\[
= \ln \left( 1 + \frac{|\mathbf{h}^H_{k,k,n}\mathbf{w}_{k,n}|^2}{\varphi_{k,n}(|\mathbf{w}, \mathbf{v}, \alpha_{k,n}|)} \right) - \ln \left( 1 + \frac{\|\mathbf{H}^H_{k,k,n}\mathbf{w}_{k,n}\|^2}{q_{k,n}(|\mathbf{w}, \mathbf{v}|)} \right)
\]

\[
= f^1_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) - f^2_{k,n}(\mathbf{w}, \mathbf{v})
\]

(10)

where

\[
f^1_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) = \ln \left( 1 + \frac{|\mathbf{h}^H_{k,k,n}\mathbf{w}_{k,n}|^2}{\varphi_{k,n}(|\mathbf{w}, \mathbf{v}, \alpha_{k,n}|)} \right)
\]

and

\[
f^2_{k,n}(\mathbf{w}, \mathbf{v}) = \ln \left( 1 + \frac{\|\mathbf{H}^H_{k,k,n}\mathbf{w}_{k,n}\|^2}{q_{k,n}(|\mathbf{w}, \mathbf{v}|)} \right).
\]

The corresponding rate in bits/sec/Hz can be calculated by evaluating

\[
\frac{\ln 2}{\ln 10} f_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n})
\]

We aim to jointly optimize the transmit beamforming vectors \(\mathbf{w}_{k,n}\), artificial noise vectors \(\mathbf{v}_k\), and the PS ratios \(\alpha_{k,n}\) for all \(k \in \mathcal{K}, n \in \mathcal{N}_k, 1 \in \mathcal{N}_{1,k}\) to maximize the worst secrecy rate of UEs

\[
\max_{\mathbf{w}_{k,n}, \mathbf{v}_k \in \mathbb{C}^{M \times 1}, \alpha_{k,n} \in (0,1)} F(\mathbf{w}, \mathbf{v}, \alpha) = \min_{k \in \mathcal{K}, n \in \mathcal{N}_k} f_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) - \frac{1}{2} \left( J_{k,n}(\mathbf{w}, \mathbf{v}, \alpha_{k,n}) - J^2_{k,n}(\mathbf{w}, \mathbf{v}) \right)
\]

(11a)

\[
\text{s.t.} \quad \sum_{n \in \mathcal{N}_k} \|\mathbf{w}_{k,n}\|^2 + \|\mathbf{v}_k\|^2 \leq P_{\text{max}}, \quad \forall k \in \mathcal{K}
\]

(11b)

\[
\sum_{k \in \mathcal{K}, n \in \mathcal{N}_k} \|\mathbf{w}_{k,n}\|^2 + \sum_{k \in \mathcal{K}} \|\mathbf{v}_k\|^2 \leq P_{\text{max}}
\]

(11c)

where

\[
p_{k,n}(\mathbf{w}, \mathbf{v}) = \sum_{n \in \mathcal{N}_k} \|\mathbf{w}_{k,n}\|^2 - \sum_{k \in \mathcal{K}} \|\mathbf{v}_k\|^2 \leq P_{\text{max}}
\]

Constraint (11b) caps the total transmit power of each BS \(k\) at a predefined value \(P_{\text{max}}\). Constraint (11c) ensures that the total transmit power of the network not exceed the allowable budget \(P_{\text{max}}\), which helps limit any potential undue interference from the considered multicell network to another network. Of course, (11c) needs to be introduced only when \(P_{\text{max}} < \sum_{k \in \mathcal{K}} P_{\text{max}}\). Constraint (11d) requires that the minimum energy harvested by UE \((k, n_1)\) be greater than some target threshold \(e_{k,n_1}^{\text{min}}\). While (11b) and (11c) are convex, the objective (11a) is not concave and the constraint (11d) is not convex due to the strong coupling between \(\mathbf{w}_{k,n}\) and \(\alpha_{k,n}\) in both the SINR-UE and EH expressions [see (4) and (6)].

\section{EH-Eavesdropper Model (Eve Model 2)}

We also consider a more practical scenario of the network internal security where any user in zone-1, UE \((k, n_1)\), \(n_1 \in \mathcal{N}_{1,k}\), may accidentally eavesdrop on the received signal of any user in zone-2, UE \((k, n_2)\), \(n_2 \in \mathcal{N}_{2,k}\). The considered case is practical because far users in zone-2 can achieve lesser information rate, compared to that achieved by the near users in zone-1, and thus are stronger potential victim of being eavesdropped upon by the near zone-1 users.\(^1\) Considering this, the signal for the zone-2 UE \((k, n_2)\) observed as an eavesdropped signal at any zone-1 UE \((k, n_1)\) in cell \(k\) is given by

\[
y_{k,n_1,n_2} = \mathbf{h}^H_{k,k,n_1} \mathbf{w}_{k,n_2} x_{k,n_2} + \mathbf{h}^H_{k,k,n_1} \left( \sum_{\bar{n} \in \mathcal{N}_k \setminus \{n_2\}} \mathbf{w}_{k,\bar{n}} x_{k,\bar{n}} + \mathbf{v}_k \right) + z_{k,n_1}
\]

(12)

Thus, the received SINR corresponding to the signal intended for the UE \((k, n_2)\) at the EV \((k, n_1)\) is given by

\[
\text{SINR-EV}_{k,n_2,n_1} = \frac{\|\mathbf{h}^H_{k,k,n_1}\mathbf{w}_{k,n_2}\|^2}{q_{k,n_2,n_1}(\mathbf{w}, \mathbf{v})}
\]

(13)

where

\[
q_{k,n_2,n_1}(\mathbf{w}, \mathbf{v}) = \sum_{n \in \mathcal{N}_k \setminus \{n_2\}} \|\mathbf{h}^H_{k,k,n_1}\mathbf{w}_{k,n}\|^2 + \sum_{k \in \mathcal{K} \setminus \{k\}} \sum_{\bar{n} \in \mathcal{N}_k} \|\mathbf{h}^H_{k,k,n_1}\mathbf{w}_{k,\bar{n}}\|^2 + \sigma_a^2
\]

(14)

Thus, the achievable secrecy rate of UE \((k, n_2)\), \(n_2 \in \mathcal{N}_{2,k}\), is given by

\[
f_{k,n_2}(\mathbf{w}, \mathbf{v}) = \ln \left( 1 + \frac{\|\mathbf{h}^H_{k,k,n_1}\mathbf{w}_{k,n_2}\|^2}{\varphi_{k,n_2}(\mathbf{w}, \mathbf{v}, 1)} \right) - \ln \left( 1 + \frac{\|\mathbf{h}^H_{k,k,n_1}\mathbf{w}_{k,n_2}\|^2}{q_{k,n_2,n_1}(\mathbf{w}, \mathbf{v})} \right)
\]

(15)

where\(\varphi_{k,n_2}(\mathbf{w}, \mathbf{v}, 1)\) is defined in (5) for \(n_2 = n_2\).\(^1\)

In such eavesdropper model, we aim to jointly optimize the transmit beamforming vectors \(\mathbf{w}_{k,n}\), artificial noise vectors \(\mathbf{v}_k\), and the PS ratios \(\alpha_{k,n}\) for all \(k \in \mathcal{K}, n \in \mathcal{N}_k, 1 \in \mathcal{N}_{1,k}\) to maximize the worst secrecy rate of UE\((k, n_2)\) among \(k\) in

\(^1\)The general cases that (i) near zone-1 users can eavesdrop on the received signal of any user either in zone-1 or zone-2 or (ii) any user in any zone can eavesdrop on the received signal of any other user in the cell can be easily obtained by slight modification of proposed system model and our extensive simulation analysis (cf. Fig. 6) study all such cases.
\[ \frac{\sum \sum \text{Trace}(W_{k,n}) + \sum \text{Trace}(V_k)}{\sum \sum \text{Trace}(W_{k,n})} \leq P_{\text{max}} \]

where the constraints (17b)-(17f) are convex. By dropping the rank-one nonconvex constraints (17g), the problem (17) is maximization of a d.c. function subject to convex constraints, which is readily solved by d.c. iterations [23], avoiding any substantial increasing the number of variables as in [19], [29]–[31]. D.C. iterations generate a feasible point \((W^{(s+1)}, V^{(s+1)}, \rho^{(s+1)}, \beta^{(s+1)})\), which is better than the incumbent \((W^{(s)}, V^{(s)}, \rho^{(s)}, \beta^{(s)})\), by solving the convex program

\[
\max_{W, V, \rho, \beta} \min_{k \in K, n \in N_k} \left[ f_{k,n}^1(W, V, \rho_{k,n}) - \frac{f_{k,n}^2(W, V, \rho_{k,n})}{\rho_{k,n}} \right]
\]

s.t. \((17b) - (17f)\).
On the other hand, by writing the rank-one constraints (17g) equivalently as
\[
\text{Trace}(W_{k,n}) - \lambda_{\max}(W_{k,n}) \leq 0, \quad k \in \mathcal{K}, n \in N_k
\]
\[
\text{Trace}(V_k) - \lambda_{\max}(V_k) \leq 0, \quad k \in \mathcal{K},
\]
where \( \lambda_{\max}(W_{k,n}) \) (resp., \( \lambda_{\max}(V_k) \)) is the maximal eigenvalue of \( W_{k,n} \) (resp., \( V_k \)), the nonconvex optimization problem (17) can be represented by the following exact penalty optimization [22]:
\[
\max_{W_{k,n}, V_{k,n}} \left\{ \min_{k \in \mathcal{K}, n \in N_k} \left[ f_{k,n}^1(W, V, \rho) - f_{k,n}^2(W, V, \rho) \right] + \mu \left[ \sum_{k \in \mathcal{K}, n \in N_k} (\lambda_{\max}(W_{k,n}) - \text{Trace}(W_{k,n})) + \sum_{k \in \mathcal{K}} (\lambda_{\max}(V_k) - \text{Trace}(V_k)) \right] \right\}
\]
\[
\text{s.t. } (17b) - (17f).
\]
for penalty parameter \( \mu > 0 \), which is again maximization of a d.c. function subject to convex constraints. By [23], (20) can be efficiently solved by d.c. iterations, which generate a feasible point \((W^{(\text{inc})}, V^{(\text{inc})}, \rho^{(\text{inc})}, \beta^{(\text{inc})})\) from the incumbent \((W^{(s)}, V^{(s)}, \rho^{(s)}, \beta^{(s)})\) by solving the convex program
\[
\max_{W, V, \rho, \beta} \left\{ \min_{k \in \mathcal{K}, n \in N_k} \left[ f_{k,n}^1(W, V, \rho_{k,n}) - f_{k,n}^2(W, V, \rho_{k,n}) \right] + \mu \left[ \sum_{k \in \mathcal{K}, n \in N_k} (\lambda_{k,n}(W_{k,n}) - \text{Trace}(W_{k,n})) + \sum_{k \in \mathcal{K}} (\lambda_{k}(V_k) - \text{Trace}(V_k)) \right] \right\}
\]
\[
\text{s.t. } (17b) - (17f).
\]
where
\[
\lambda_{k,n}(W_{k,n}) = \lambda_{\max}(W_{k,n}) + (\tilde{w}_{k,n}^{(s)})^H (W_{k,n} - W_{k,n}^{(s)}) \tilde{w}_{k,n}^{(s)},
\]
\[
\lambda_{k}(V_k) = \lambda_{\max}(V_k) + (\tilde{v}_k^{(s)})^H (V_k - V_k^{(s)}) \tilde{v}_k^{(s)},
\]
and \( \tilde{w}_{k,n}(\tilde{v}_k^{(s)}) \) (resp.) is the normalized eigenvector corresponding to \( \lambda_{\max}(W_{k,n}) \) (resp., \( \lambda_{\max}(V_k) \)). The sequence \( \{W^{(s)}, V^{(s)}, \rho^{(s)}, \beta^{(s)}\} \) is of iteratively improved feasible points to (20), which converges to an optimal rank-one solution of (17).

Problem (16) can be similarly treated. However, the main drawback of this approach is that the total dimension of the variables \( W \) and \( V \) increases explosively that makes the iteration (21) computationally expensive. Also, there is no beforehand choice for the penalty parameter \( \mu \) to speed up the convergence of iterations (21).

In the following subsections, we propose path-following optimization algorithms to solve the secrecy rate problems (11) and (16) directly in the beamforming variables \( W \) and \( V \). Each iteration is a simple convex quadratic program in \( W \) and \( V \), so its computation is very efficient.

A. Proposed Solution for Problem (11) (Eve Model 1)

In order to propose path-following iterations for solution of (11) we find a concave lower bound approximation for the objective function \( F(w, v, \alpha) \) in (11a) and inner convex approximation for the EH constraint (11d).

Let us first find the concave lower bound approximation of \( f_{k,n}^1(w, v, \alpha_{k,n}) - f_{k,n}^2(w, v) \) at \( \text{th} \) iteration. Thus, we need to develop a lower bounding concave function for the first term \( f_{k,n}^1(w, v, \alpha_{k,n}) \) and upper bounding convex function for the second term \( f_{k,n}^2(w, v) \), which agree with these terms at \( (w^{(s)}, v^{(s)}, \alpha^{(s)}_{k,n}) \) of \( \text{th} \) iteration.

Proposition 1: The lower bounding concave approximation for \( f_{k,n}^1(w, v, \alpha_{k,n}) \) is given by
\[
f_{k,n}^1(w, v, \alpha_{k,n}) \geq f_{k,n}^1(w, v, \alpha_{k,n})
\]
\[
\geq f_{k,n}^1(w^{(s)}, v^{(s)}, \alpha_{k,n}) + 2 \begin{bmatrix}
\mathbb{H}_{k,n}^H h_{k,n} h_{k,n}^H (w_{k,n} - w_{k,n}^{(s)}) \\
\varphi_{k,n}(w_{k,n}, v_{k,n}, \alpha_{k,n}) + \mathbb{H}_{k,n}^H \mathbb{H}_{k,n} \|w_{k,n} - w_{k,n}^{(s)}\|^2
\end{bmatrix}
\]
\[
\text{s.t. } (22a).
\]
and upper bounding convex approximation for \( f_{k,n}^2(w, v) \) is given by
\[
f_{k,n}^2(w, v) \leq f_{k,n}^2(w, v)
\]
\[
\leq f_{k,n}^2(w^{(s)}, v^{(s)}) + \begin{bmatrix}
1 + \frac{\mathbb{H}_{k,n}^H w_{k,n}^{(s)}}{q_{k,n}(w^{(s)}, v^{(s)})} \\
\mathbb{H}_{k,n}^H w_{k,n}^{(s)}
\end{bmatrix}^{-1}
\]
\[
\times \left[ \begin{bmatrix}
\|w_{k,n} - w_{k,n}^{(s)}\| \\
q_{k,n}(w_{k,n}^{(s)}, v^{(s)}), w_{k,n}^{(s)}
\end{bmatrix}^2
\end{bmatrix}
\]
\[
\text{s.t. } (23a).
\]
\[
f_{k,n}^2(w^{(s)}, v^{(s)}) - 1
\]
\[
+ \begin{bmatrix}
1 + \frac{\mathbb{H}_{k,n}^H w_{k,n}^{(s)}}{q_{k,n}(w^{(s)}, v^{(s)})} \\
\mathbb{H}_{k,n}^H w_{k,n}^{(s)}
\end{bmatrix}^{-1}
\]
\[
\times \left[ \begin{bmatrix}
\|w_{k,n} - w_{k,n}^{(s)}\| \\
q_{k,n}(w_{k,n}^{(s)}, v^{(s)}), w_{k,n}^{(s)}
\end{bmatrix}^2
\end{bmatrix}
\]
\[
\text{s.t. } (23b).
\]
where function
\[ \|H^h_{k,n} w_{k,n}\|^2 \]
\[ q_{k,n}^{(e)}(w, \nu) \]
\[ q_{k,n}^{(e)}(w, \nu) \geq 0. \] (25)

The functions \( f_{k,n}^{1,(e)} \) and \( f_{k,n}^{2,(e)} \) agree with \( f_{k,n}^{1} \) and \( f_{k,n}^{2} \), respectively, at \((w_{k,n}, \nu^{(e)}_{k,n}, \alpha^{(e)}_{k,n})\).

Proof: See Appendix A.

Next, we have to find an inner convex approximation for the EH constraint (11d) in the sense that any point that is feasible for the former is also feasible for the latter. This requires us to find an affine approximation of \( pk_{n}^{(e)}(w, \nu) \) at the \( k \)th iteration, which is given by
\[ p_{k,n}^{(e)}(w, \nu) = \sum_{k \in K} \sum_{n \in N_k} \Re\{H^k_{h,k,n} w_{k,n}^{(e)} + H^k_{h,k,n} w_{k,n}^{(e)} - H^k_{h,k,n} w_{k,n}^{(e)}\} \]
\[ + \sum_{k \in K} \Re\{H^k_{h,k,n} v_{k}^{(e)} + H^k_{h,k,n} v_{k}^{(e)} - H^k_{h,k,n} v_{k}^{(e)}\} + \sigma^2. \] (26)

Using (26), an inner convex approximation for the EH constraint (11d) is given by
\[ p_{k,n}^{(e)}(w, \nu) - e_{k,n}^{\min}/\zeta_{k,n}(1 - \alpha_{k,n}) \geq 0, \forall k \in K, n \in N_{1,k}, \] (27)
where (27) is inner convex approximation of (11d) in the sense that each feasible point to the former is also feasible for the latter and provides a lower bound for the optimal value of the former. Using (22b), (11b), (11c), (25) and (27), the \( \kappa \)-iteration for the nonconvex problem (11) is the following inner convex approximation:
\[ \max_{w_{k,n}, \nu_{k,n} \in M \times K, \alpha_{k,n} \in (0,1)} F^{(e)}(w, \nu, \alpha) \]
\[ \triangleq \min_{k \in K, n \in N_k} [f_{k,n}^{1,(e)}(w, \nu, \alpha_{k,n}) - f_{k,n}^{2,(e)}(w, \nu)] \]
\[ \text{s.t. (11b), (11c), (25), (27),} \] (28a)

where the details for finding the initial feasible point \( (w_{k,n}^{(0)}, \nu_{k,n}^{(0)}, \alpha_{k,n}^{(0)}) \), \( \forall k \in K, n \in N_k, n_1 \in N_{1,k} \) are given in the following subsection.

1) Initialization of Algorithm 1: The initial feasible point, \( (w_{k,n}^{(0)}, \nu_{k,n}^{(0)}, \alpha_{k,n}^{(0)}) \), \( \forall k \in K, n \in N_k, n_1 \in N_{1,k} \), is obtained by solving a feasibility program which in addition to power constraints, (11b), (11c), and energy harvesting constraint (11d), also aims to satisfy a minimum threshold SINR, \( \gamma_{\min} \) for all UEs (\( k, n \)), \( \forall k \in K, n \in N_k \). The satisfaction of SINR constraint,
\[ h_{k,n}^{H} w_{k,n} \leq \gamma_{\min} \nu_{k,n}(w, \nu, \alpha_{k,n}), \forall k \in K, n \in N_k, \] (29)
during initialization assists the quick convergence of Algorithm 1. Constraint (29) is nonconvex due to coupling between \( w_{k,n} \) and \( \alpha_{k,n} \). Let us express it as second order cone (SOC) constraint. For \( \bar{w}_{k,n} = e^{-j\arg(h_{k,n}^{H} w_{k,n})} w_{k,n} \), one has \( |h_{k,n}^{H} w_{k,n}| = h_{k,n}^{H} \bar{w}_{k,n} = \Re\{h_{k,n}^{H} \bar{w}_{k,n}\} \geq 0 \) and \( |h_{k,n}^{H} w_{k,n}| = |h_{k,n}^{H} \bar{w}_{k,n}| \) for \( (k', n') \neq (k, n) \), where \( j = \sqrt{-1} \). By making the variable change \( \alpha_{k,n} \rightarrow \alpha_{k,n}^{2} \), in (29), we have the following SOC constraint [37]:
\[ \Re\{h_{k,n}^{H} \bar{w}_{k,n}\} \geq \sqrt{\gamma_{\min}} \nu_{k,n}(w, \nu, \alpha_{k,n}^{2}), \forall k \in K, n \in N_k, \] (30)
which is equivalent to the following SOC:
\[ \Re\{h_{k,n}^{H} \bar{w}_{k,n}\} \geq \sqrt{\gamma_{\min}} \] (31)
\[ (t_{k,n}^{(0)}, 1/\alpha_{k,n}) \geq 0, \forall k \in K, n_1 \in N_{1,k}, \] (32)
where \( \alpha_{k,n}^{2} \) is an \((N-1)\times 1\) column vector, \( t_{k,n}^{(0)} \) is an auxiliary variable, and
\[ \mu_{k,n} = \begin{cases} \sigma, & n \in N_{1,k} \\ \gamma_c, & n \in N_{2,k} \end{cases} \]

Meanwhile, under the variable change \( \alpha_{k,n} \rightarrow \alpha_{k,n}^{2} \), in (27), the harvested energy constraint (11d) is implied by the following constraint in \( \alpha_{k,n}^{2} \) and a slack variable \( \beta_{k,n}^{2} \):
\[ \sqrt{\min_{k \in K, n \in N_k} \zeta_{k,n}/\beta_{k,n}^{2}} - \Re\{h_{k,n}^{H} w_{k,n}\} \leq 0, \forall k \in K, n_1 \in N_{1,k} \] (33a)
\[ \beta_{k,n}^{2} + \alpha_{k,n}^{2} \leq 1, \forall k \in K, n_1 \in N_{1,k}. \] (33b)

Thus, initial feasible point, \( (w_{k,n}^{(0)}, \nu_{k,n}^{(0)}, \alpha_{k,n}^{(0)}) \), \( \forall k \in K, n \in N_k, n_1 \in N_{1,k} \), of (11) is obtained by solving a feasibility program (11b), (11c), (31), (32), (33a), and (33b). In Algorithm 1, we summarize our proposed path-following optimization algorithm to solve the EH constrained secrecy rate problem (11).

Proposition 2: Algorithm 1 generates a sequence \( \{(w^{(k)}, \nu^{(k)}, \alpha^{(k)})\} \) of improved points of (11), which converges to a Karush-Kuhn-Tucker (KKT) point.
Algorithm 1 Path-following Iterations for Problem (11)

1: Initialize \( \kappa := 0. \)
2: Choose a feasible point \( \left( w_{k,n}^{(0)}, v_{k,n}^{(0)}, \alpha_{k,n}^{(0)} \right), \forall k \in K, n \in \mathcal{N}_k, n_1 \in \mathcal{N}_{1,k} \) of (11) by solving a feasibility program (11b), (11c), (31), (32), (33a), and (33a).
3: repeat
4: Solve (38) for \( \left( w_{k,n}^{(\kappa+1)}, v_{k,n}^{(\kappa+1)}, \alpha_{k,n}^{(\kappa+1)} \right), \forall k \in K, n \in \mathcal{N}_k. \)
5: Set \( \kappa := \kappa + 1. \)
6: until convergence of the objective in (11).

Proof: We have

\[
F(w, v, \alpha) \geq F(\alpha)(w, v, \alpha) \forall w, v, \alpha.
\]

Therefore,

\[
F(w^{(\kappa+1)}, v^{(\kappa+1)}, \alpha^{(\kappa+1)}) \geq F(\alpha^{(\kappa+1)}) = F(w^{(\kappa)}, v^{(\kappa)}, \alpha^{(\kappa)}),
\]

where the second inequality follows from the fact that \( (w^{(\kappa+1)}, v^{(\kappa+1)}, \alpha^{(\kappa+1)}) \) and \( (w^{(\kappa)}, v^{(\kappa)}, \alpha^{(\kappa)}) \) are the optimal solution and a feasible point of (11), respectively. This result shows that \( (w^{(\kappa+1)}, v^{(\kappa+1)}, \alpha^{(\kappa+1)}) \) is a better point to (11) than \( (w^{(\kappa)}, v^{(\kappa)}, \alpha^{(\kappa)}) \). Furthermore, the sequence \( \{(w^{(\kappa)}, v^{(\kappa)}, \alpha^{(\kappa)})\} \) is bounded by constraints (11b) and (11c). By Cauchy’s theorem\(^2\), there is a convergent subsequence \( \{(w^{(\kappa)}, v^{(\kappa)}, \alpha^{(\kappa)})\} \) with a limit point \( (w, v, \tilde{\alpha}) \), i.e.,

\[
\lim_{\nu \to +\infty} \left[ F(w^{(\kappa)}, v^{(\kappa)}, \alpha^{(\kappa)}) - F(w, v, \tilde{\alpha}) \right] = 0.
\]

For every \( \nu \) such that \( \kappa_\nu \leq \kappa \leq \kappa_{\nu+1} \), so

\[
0 = \lim_{\nu \to +\infty} \left[ F(w^{(\kappa)}, w^{(\kappa)}, \alpha^{(\kappa)}) - F(w, w, \tilde{\alpha}) \right]
= \lim_{\nu \to +\infty} \left[ F(w^{(\kappa)}, \alpha^{(\kappa)}) - F(w, \tilde{\alpha}) \right]
\leq \lim_{\nu \to +\infty} \left[ F(w^{(\kappa)}, \alpha^{(\kappa)}) - F(w, \tilde{\alpha}) \right]
= 0,
\]

which shows that \( \lim_{\kappa \to \infty} F(w^{(\kappa)}, \alpha^{(\kappa)}) = F(w, \tilde{\alpha}). \)

Each accumulation point \( \{(w, v, \tilde{\alpha})\} \) of the sequence \( \{(w^{(\kappa)}, v^{(\kappa)}, \alpha^{(\kappa)})\} \) is a KKT-point according to [38, Theorem 1].

B. Proposed Solution for Problem (16) (Eve Model 2)

To propose path-following optimization for solution of (16), we find a concave lower bound approximation for the objective function \( F(w, v, \alpha_k) \) in (16a) and inner convex approximations for the SINR (16b) and EH constraints (11d).

Let us first find a concave approximation of \( \bar{f}_{k,n_2}^1(w, v) - \bar{f}_{k,n_2}^2(w, v) \) at \( (w^{(\kappa)}, v^{(\kappa)}) \) of \( \kappa \)th iteration. We can use Proposition 1 to find a lower bounding concave function for the first term \( \bar{f}_{k,n_2}^1(w, v) \) and upper bounding convex function for the second term \( \bar{f}_{k,n_2}^2(w, v) \). Thus, a lower bounding concave approximation for \( \bar{f}_{k,n_2}^1(w, v) \) is given by

\[
\ln \left( 1 + \frac{|h_{k,n_2}^H w_{k,n_2}|^2}{\varphi_{k,n_2}(w, v, 1)} \right) = \bar{f}_{k,n_2}^1(w, v)
\]

and an upper bounding convex approximation for \( \bar{f}_{k,n_2}^2(w, v) \) is given by

\[
\bar{f}_{k,n_2}^2(w, v) \leq \bar{f}_{k,n_2}^2(w, v)
\]

with

\[
q_{k,n_2,n_1}(w, v) = \sum_{\tilde{n} \in \mathcal{N}_k \setminus \{n_2\}} \mathbb{R}\{h_{k,n_1}^H \bar{w}_{k,n_1} \},
\]

where the function \( q_{k,n_2,n_1}(w, v) \) is convex on domain

\[
q_{k,n_2,n_1}(w, v) \geq 0.
\]

\(^2\)From a bounded (compact) sequence, there is a convergent subsequence
Next, we are left with SINR constraint (16b) and EH constraint (11d). By making the variable change $\alpha_{k,n_1} \rightarrow \alpha_{k,n_1}^2$, the SINR constraint (16b) is equivalent to the SOC constraint (31) and (32). Finally, by using the affine approximation of $p_{k,n_1}(w,v)$, given by $p_{k,n_1}^{(\kappa)}(w,v)$ in (26), and applying the variable change $\alpha_{k,n_1} \rightarrow \alpha_{k,n_1}^2$ in the constraint (27), an inner convex approximation for the EH constraint (11d) for Problem (16) is given by

\[
p_{k,n_1}^{(\kappa)}(w,v) - \frac{e_{k,n_1}^{\min}}{\zeta_{k,n_1} / \beta_{k,n_1}} \geq 0, \forall k \in \mathcal{K}, n_1 \in \mathcal{N}_{1,k},
\]

\[
\beta_{k,n_1} + \alpha_{k,n_1}^2 \leq 1, \beta_{k,n_1} > 0, \forall k \in \mathcal{K}, n_1 \in \mathcal{N}_{1,k}, \tag{38b}
\]

Using (34), (11b), (11c), (37), (31), (32), (38a), and (38b), the $\kappa$-iteration for (16) is given by its following inner approximated optimization problem:

\[
\max_{w_{k,n}, v_{k,n} \in \mathbb{C}^{M+1}, \alpha_{k,n_1} \in (0,1), \beta_{k,n_1}} E^{(\kappa)}(w, v)
\]

\[
\phi \triangleq \min_{n \in \mathcal{N}_k} \left[ f_{k,n_1}^{(1,\kappa)}(w,v) - f_{k,n_2}^{(2,\kappa)}(w,v) \right]
\]

s.t. (11b), (11c), (37), (31), (32), (38a), (38b).

In Algorithm 2, we summarize our proposed path-following optimization algorithm to solve the Problem (16), where the same initialization as detailed in Section III-A1 can be used to find the initial feasible point $\left( w_{k,n}^{(0)}, v_k^{(0)}, \alpha_{k,n_1}^{(0)} \right)$, $\forall k \in \mathcal{K}, n \in \mathcal{N}_k, n_1 \in \mathcal{N}_{1,k}$ for the Problem (16).

Analogously to Proposition 1, it can be shown that Algorithm 2 generates a sequence $\{ (w^{(k)}, v^{(k)}, \alpha^{(k)}_{k,n_1}) \}$ of improved points of (16), which converges to a KKT point.

IV. NUMERICAL EXAMPLES

Fig. 2 shows the network topology with $K = 3$ cells and $N = N_k = 4$, $\forall k \in \mathcal{K}$ UEs per cell that we use in our numerical examples. Out of the four users in each cell, two are placed inside the inner-circle and two inside the outer-zone, i.e., $\mathcal{N}_{1,k} = \mathcal{N}_{2,k} = 2$, $\forall k$. We set the cell radius as 40m and the BS-to-UE distance is 7 m and 20 m in the inner and outer zone of each cell, respectively. We assume that a single $N_e = 2$-antennas eavesdropper is randomly placed in each cell inside the inner circle. In our simulation setup, their placements are at 5 m, 10 m, and 15 m from the respective BSs in three cells as shown in Fig. 2. We set the path loss exponent as $\beta = 3$. For small-scale fading, we generate Rician fading according to Rician factor, $K_R = 10$ dB [39]. For simplicity and without loss of generality, we assume that the minimum energy harvesting requirement $e_{k,n_1}^{\min} = e^{\min}$ and the energy harvesting efficiency $\zeta_{k,n_1} = \zeta$, $\forall k, n_1$ (for UEs inside inner circle). In all simulations, we set $\zeta = 0.5$, $\sigma_0^2 = -90$ dBm, and $\sigma_e^2 = -90$ dBm. We further set the maximum power of each BS as $P_k^{\max} = 26$ dBm, which is consistent with the power budget usually assumed for small-cell BSs [40], and we set the maximum power budget for the whole network to be $P^{\max} = 30$ dBm. For Problem (16), we set the minimum threshold SINR for users in the inner zone to be $\gamma_{\min} = 6$ dB.

Fig. 3 shows the convergence of our proposed Algorithms 1 and 2 for $M = 5$ and $e^{\min} = -20$ dBm.

Algorithm 2 Path-following iterations for Problem (16)

1: Initialize $\kappa := 0$.
2: Choose a feasible point $\left( w_{k,n}^{(0)}, v_k^{(0)}, \alpha_{k,n_1}^{(0)} \right)$, $\forall k \in \mathcal{K}, n \in \mathcal{N}_k, n_1 \in \mathcal{N}_{1,k}$ of (16) by solving a feasibility program (11b), (11c), (31), (32), (33a), and (33a).
3: repeat
4: Solve (39) for $\left( w_{k,n}^{(\kappa+1)}, v_k^{(\kappa+1)}, \alpha_{k,n_1}^{(\kappa+1)} \right)$, $\forall k \in \mathcal{K}, n \in \mathcal{N}_k$.
5: Set $\kappa := \kappa + 1$.
6: until convergence of the objective in (16).

Figure 2. Topology of the multicell network used in numerical examples

Figure 3. Convergence of Algorithms 1 and 2 for $M = 5$ and $e^{\min} = -20$ dBm.
2 just took 7 iterations to converge. On average over large number of channel realizations, we found that Algorithm 1 requires 16 and Algorithm 2 requires 12 iterations before convergence. Fig. 3 also shows that achievable worst user secrecy rate for Eve Model 1 is smaller than that for Eve Model 2. This is expected since we employ multi-antenna single eavesdropper in Eve Model 1, which decreases the achievable secrecy rate.

Figs. 4 and 5 plot the worst user secrecy rate and worst user normal rate (without eavesdroppers) for Eve model 1 as detailed in Section II-A. Basically, secrecy rate in the presence of eavesdroppers refers to the Problem (11) and the proposed solution is in Algorithm 1. We compare the achievable secure rate for our proposed Algorithm 1 with the normal rate which assumes no presence of eavesdroppers and thus solve Problem (11) in the absence of the factor $f_{k,n}^S(w,v)$ in (11a). The particular result is labeled as “Algorithm 1 (without EV).”

Fig. 4 plots the rate (in bits/sec/Hz) for varying number of antennas $M = \{3, 4, 5, 6\}$ with fixed energy harvesting threshold $e_{\text{min}} = -20$ dBm, while Fig. 5 plots the rate (in bits/sec/Hz) for varying range of energy harvesting targets $e_{\text{min}} = \{-25, -23, \ldots, -15\}$ dBm with fixed number of antennas at the BS $M = 5$. Fig. 4 shows that the rate is almost linearly increasing with number of antennas from 3 to 6. Fig. 5 shows that rate decreases by increasing the EH targets, which does make sense as more power is required for EH to achieve a high EH target, which decreases the available power for information decoding and so does the same to the information rate. Fig. 4 also compares the performance of the proposed Algorithm 1 with the one which employs exact-penalty iterations in (21). We can observe that the performance of the proposed Algorithm 1 is quite close to that of the exact-penalty iteration based algorithm. It is important to note that the proposed Algorithm 1 is computationally quite
also compares the performance of the proposed Algorithm 2 as that was observed in Figs. 4 and 5 for Eve Model 1.

Figure 6 plots the rate (in bits/sec/Hz) for varying number of antennas at the BS
e

ten antennas in zone-2 to eavesdrop, but their received signal strength are quite close. This is because though case (ii) also allows far

Figure 8 plots the rate (in bits/sec/Hz) for varying number of antennas

seen in Figs. 4 and 5 for Eve Model 1. Fig. 6 also compares the performance of the proposed Algorithm 2 with general system models, (i) zone-1 UE eavesdrops on any UE and (ii) any UE can eavesdrop on any other UE in the cell. As expected, in the presence of more eavesdroppers or more victims of eavesdropping, the achievable secrecy rate under such general cases is slightly worse than that of the detailed case in Section II-B, where zone-1 UE eavesdrops on the received signal of zone-2 UE. We can also observe from Fig. 6 that secrecy rate of above mentioned general cases (i) and (ii) are quite close. This is because though case (ii) also allows far users in zone-2 to eavesdrop, but their received signal strength is quite low to ensure meaningful eavesdropping.

Fig. 8 plots the optimal average power splitting ratio versus energy harvesting threshold $e_{\text{min}}$ for fixed number of BS antennas $M = 5$, while employing both Eavesdropper Models 1 and 2.

better because exact-penalty iteration based algorithm requires complex matrix optimization and quite lot of iterations, 40 on average, to converge. On the other hand, the proposed Algorithm 1 requires only vector optimization and about 16 iterations, on average, to converge.

The computational complexities of Algorithm 1 and exact-penalty iteration based algorithm are $O(i_{A1} K^3(MN + M + N_1)^3 (K(N + 2N_1 + 1) + 1))$ and $O\left(i_{EP}\right) ((M(M + 1)/2)K(N + 1) + 2KN_1)^3 (5KN_1 + K(N + 2) + 1)$, respectively [41]. Here, $i_{A1} = 16$ is the average number of times that (28) is solved by Algorithm 1 and $i_{EP} = 40$ is the average number of times that an exact penalty algorithm (21) is solved by . Table I shows the average number of iterations, scalar variables, and linear, quadratic, and SD constraints, required by both algorithms. We can observe that proposed Algorithm 1 requires fewer constraints and variables.

Figs. 6 and 7 plot the worst user secrecy rate and worst user normal rate (without eavesdroppers) for Eve model 2 as detailed in Section II-B (see proposed Algorithm 2). Fig. 6 plots the rate (in bits/sec/Hz) for varying number of antennas $M = \{3, 4, 5, 6\}$ with fixed energy harvesting threshold $e_{\text{min}} = -20$ dBm, while Fig. 7 plots the rate (in bits/sec/Hz) for varying range of energy harvesting targets $e_{\text{min}} = \{-25, -23, \ldots, -15\}$ dBm with fixed number of antennas at the BS $M = 5$. We observe the same rate behavior as that was observed in Figs. 4 and 5 for Eve Model 1. Fig. 6 also compares the performance of the proposed Algorithm 2 with general system models, (i) zone-1 UE eavesdrops on any UE and (ii) any UE can eavesdrop on any other UE in the cell. As expected, in the presence of more eavesdroppers or more victims of eavesdropping, the achievable secrecy rate under such general cases is slightly worse than that of the detailed case in Section II-B, where zone-1 UE eavesdrops on the received signal of zone-2 UE. We can also observe from Fig. 6 that secrecy rate of above mentioned general cases (i) and (ii) are quite close. This is because though case (ii) also allows far users in zone-2 to eavesdrop, but their received signal strength is quite low to ensure meaningful eavesdropping.

Fig. 8 plots the optimal average power splitting ratio versus energy harvesting threshold $e_{\text{min}}$ for fixed number of BS antennas $M = 5$. The average has been taken among optimized PS values of all users over many channel realizations. Fig. 8 shows that on average, PS ratio decreases by increasing the energy harvesting threshold, which does make sense as $\sqrt{1 - \alpha_{k,n_1} y_{k,n_1}}$ of the received signal is processed by an EH receiver. Thus, increasing $e_{\text{min}}$ implies larger values of $1 - \alpha_{k,n_1}$ or smaller values of the PS ratio $\alpha_{k,n_1}$. In addition, Fig. 8 also shows that for Eve Model 1, we require quite larger value of PS ratios compared to that required for Eve Model 2. This is because of the multi-antenna stronger eavesdropper in Eve Model 1, which demands a larger value of $\alpha_{k,n_1}$ to boost the received signal $\sqrt{\alpha_{k,n_1} y_{k,n_1}}$, strength fed to the ID receiver and to enable the maximization of the worst user secrecy rate.

Fig. 9 plots the worst user secrecy rate for Eve model 1 for fixed number of BS antennas $M = 6$ and EH threshold $e_{\text{min}} = -15$ dBm, while employing Eavesdropper Model 1.

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>avg. # iter</th>
<th>scal var</th>
<th>lin cons</th>
<th>quad cons</th>
<th>SD cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alg. 1</td>
<td>16</td>
<td>$O(1) + 2KN_1 + 1)$</td>
<td>$O(K(N + 1) + KN_1 + K + 1)$</td>
<td>$O(KN_1 + 1)$</td>
<td>$O(K)$</td>
</tr>
<tr>
<td>Exact penalty Alg.</td>
<td>40</td>
<td>$(M(M + 1)/2)K(N + 1) + 2KN_1$</td>
<td>$5KN_1 + K + 1$</td>
<td>$2KN_1$</td>
<td>$K(N + 1)$</td>
</tr>
</tbody>
</table>

Table I

Complexity analysis for Alg. 1 and exact penalty algorithm in Section III to solve Problem (11)
This means for \( f \) of our proposed algorithms. For more details, please refer to the full paper for a comprehensive explanation.
Ali Arshad Nasir (S09-M13) is an Assistant Professor in the Department of Electrical Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, KSA. Previously, he held the position of Assistant Professor in the School of Electrical and Computer Engineering (SEECS) at National University of Sciences & Technology (NUST), Pakistan, from 2015-2016. He received his Ph.D. in telecommunications engineering from the Australian National University (ANU), Australia in 2013 and worked there as a Research Fellow from 2012-2015. His research interests are in the area of signal processing in wireless communication systems. He is an Associate Editor for IEEE Canadian Journal of Electrical and Computer Engineering.

Hoang Duong Tuan received the Diploma (Hons.) and Ph.D. degrees in applied mathematics from Odessa State University, Ukraine, in 1987 and 1991, respectively. He spent nine academic years in Japan as an Assistant Professor in the Department of Electronic-Mechanical Engineering, Nagoya University, from 1994 to 1999, and then as an Associate Professor in the Department of Electrical and Computer Engineering, Toyota Technological Institute, Nagoya, from 1999 to 2003. He was a Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, from 2003 to 2011. He is currently a Professor with the Centre for Health Technologies, University of Technology Sydney. He has been involved in research with the areas of optimization, control, signal processing, wireless communication, and biomedical engineering for more than 20 years.

Trung Q. Duong (S’05, M’12, SM’13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen’s University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include physical layer security, energy-harvesting communications, cognitive relay networks. He is the author or co-author of more than 220 technical papers published in scientific journals (110 articles) and presented at international conferences (110 papers).

Dr. Duong currently serves as an Editor for the IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, IEEE Communications Letters, IET Communications. He was a Editor of Wiley Transactions on Emerging Telecommunications Technologies, Electronics Letters and has also served as the Guest Editor of the special issue on some major journals including IEEE Journal in SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE ACCESS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2016-2021).

Vincent Poor (S72, M77, SM82, F87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering. From 2006 till 2016, he served as Dean of Princeton’s School of Engineering and Applied Science. Dr. Poor’s research interests are in the areas of statistical signal processing, stochastic analysis and information theory, and their applications in wireless networks and related fields. Among his publications in these areas is the recent book Mechanisms and Games for Dynamic Spectrum Allocation (Cambridge University Press, 2014).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, and a foreign member of the Royal Society. He is also a Fellow of the American Academy of Arts and Sciences and the National Academy of Inventors, and of other national and international academies. He received the Technical Achievement and Society Awards of the IEEE Signal Processing Society in 2007 and 2011, respectively. Recent recognition of his work includes the 2014 URSI Booker Gold Medal, the 2015 EURASIP Athanasios Papoulis Award, the 2016 John Fritz Medal, and honorary doctorates from Aalborg University, Aalto University, HKUST and the University of Edinburgh.