Energy-Efficient Resource Optimization with Wireless Power Transfer for Secure NOMA Systems

Lei Lei[1], Zheng Chang[2], Yun Hu[3], Tapani Ristaniemi[2], Yaxiong Yuan[1], and Symeon Chatzinotas[1]

[1]Interdisciplinary Centre for Security, Reliability and Trust, Luxembourg University, Luxembourg
[2]Department of Mathematical Information Technology, University of Jyväskylä, Jyväskylä, Finland
[3]Xidian University, Xi'an, China
Emails: {lei.lei; symeon.chatzinotas}@uni.lu, {zheng.chang; tapani.ristaniemi}@jyu.fi, huyun@xidian.edu.cn

***Abstract*—In this paper, we investigate resource allocation algorithm design for secure non-orthogonal multiple access (NOMA) systems empowered by wireless power transfer. With the consideration of an existing eavesdropper, the objective is to obtain secure and energy efficient transmission among multiple users by optimizing time, power and subchannel allocation. Moreover, we also take into consideration for the practical case that the statistics of the channel state information of the eavesdropper is not available. In order to address the optimization problem and its high computational complexity, we propose an iterative algorithm with guaranteed convergence to deliver a suboptimal solution for general cases. For some special cases, the solution ensures the global optimum. Numerical studies demonstrate the competitiveness of the proposed algorithmic solution over conventional orthogonal multiple access systems as well as over other existing NOMA resource allocation schemes.**

***Index Terms*—Non-orthogonal multiple access (NOMA), security, wireless power transfer, subchannel allocation, power allocation**

I. Introduction

Non-orthogonal multiple access (NOMA) has received significant attention for the fifth generation (5G) communication systems [1]–[3]. To solve the energy supplement problem and increase the energy efficiency (EE) of NOMA systems, energy harvesting technology is considered as one of promising solutions. Compared with conventional energy sources such as wind and solar, electromagnetic signals are not location-dependent. Therefore, network elements may experience difficulty in accessing conventional energy source. Simultaneous wireless information and power transfer (SWIPT) emerges as an effective way for energy supply. As electromagnetic signals are almost everywhere, SWIPT research recently attracts considerable interests from the academic and industrial communities [4], [5]. In addition to the energy consumption issues, security of the cellular system is also critical as the traditional wireless communications may be vulnerable to increased security threats. Among the design of security mechanisms, physical-layer (PHY) security (PLS) has emerged as a research topic due to its independence of the interception ability of eavesdroppers. The basic idea for enhancing PLS is to exploit the randomness of wireless channel for secure data transmission. Thus, how to design the secure transmission from the PHY perspective is also of significance for the future wireless networks. PLS has been studied in various scenarios [6], [7], but there is still a paucity of research contributions on investigating the security issues of NOMA, which motivates to investigate the PLS in the NOMA system. Note that the unique features of NOMA makes the analysis of the PLS of NOMA different from that of OMA. However, due to the broadcast nature of the wireless communication, if privacy information is contained in the transmission signals, there still be a chance that passive eavesdropping from external/internal eavesdroppers may occur in NOMA, which motivates us to design corresponding algorithm to enhance the PLS of NOMA.

In this paper, with the objective to ensure the secure rate and energy efficiency, we address a resource allocation problem for NOMA systems with wireless power transfer. The contribution of this work can be summarized as follows. Firstly, we study the EE optimization with considering secrecy data rate for a multiple-antenna multi-user NOMA system empowered by wireless power transfer (WPT). With the objective to obtain the optimal EE with secrecy rate, we jointly optimize power allocation, time allocation, and subchannel allocation, and formulate the optimization problem as well. Secondly, in the considered system, the whole time slot T is divided into WPT time and wireless information transfer (WIT) time. We propose a time allocation scheme to determine the optimal time allocation, along with a scheme to jointly optimize power and subchannel allocations. Thirdly, we consider the practical case that the CSI of the eavesdropper cannot be fully obtained by the legitimate nodes of the system. Instead, we investigate the system performance under the consideration to estimate the secrecy rate, based on derived thorough theoretical analysis. Lastly, the formulated optimization problem is nonconvex and contains combinatorial components. To address it, we reformulate the nonconvex problem, decompose the difficult constrains by transformation. We develop an iterative algorithm providing promising results, in terms of global optimal or suboptimal solutions, for solving the problem. The performance evaluation demonstrates the superior performance compared with previously proposed scheme.

II. System Model

We consider a wireless network consisting of one energy transmitter (EnT) with $N_T > 1$ antennas, K energy harvesting receivers (EHRs) with $N_R > 1$ antennas and an eavesdropper with $N_E \geq 1$ antennas. The EnT is able to charge the EHRs via WPT. After charging, the EHR can utilize the

received energy and then transmit the information data to the EnT. Correspondingly, in the WIT phrase, the EHRs become information transmitter (InTs) and the EnT becomes the information receiver (InR). In the following, InT and EHR, EnT and InR are used interchangeably. For security concerns, we assume $N_R > N_E$, i.e., $N_E = N_R - 1$ in this work. Meanwhile, the eavesdropper can passively overhearing the information data. The overall bandwidth B is divided into N subchannels, each with bandwidth $W = B/N$. The set of subchannels is denoted as $\mathcal{N}$ and the set of users that uses subchannel n is denoted as $\mathcal{U}_n$. We assume that the channel state information (CSI) between the EnT/InR and EHRs/InTs are perfectly known, but the one of the eavesdropper is unknown. With successive interference cancellation (SIC), some of the co-channel interference will be treated as decodable signals instead of as additive noise.

A. Wireless Power Transfer and Data Transmission

We consider a quasi-static block fading channel model where the channel between the transmitter and receiver is constant for a given transmission block T. We assume that the whole transmission process including WPT and WIT phrases. In the first time slot τT, the EnT charges EHR k via WPT and the EHR stores the harvested energy in a rechargeable battery. Then, in the time duration $(1-\tau)T$, EHR k becomes the InT and sends its own data to the EnT/InR. Considering the devices are equipped with wireless energy harvesting capability, the energy harvested by EHR k on subchannel n can be considered as follows [8],

$$E_{k,n} = \vartheta \tau T P_n |\mathbf{B}_{k,n}^H \mathbf{H}_{k,n}|^2 = \vartheta \tau T P_n \|\mathbf{H}_{k,n}\|^2 \quad (1)$$

where τ is the time fraction of WPT. P_n is the transmit power of the EnT on subchannel n. $\mathbf{H}_{k,n}$ is the channel coefficient matrix from the EnT to the EHR k on subchannel n. $0 < \vartheta < 1$ is the receiver efficiency of WPT, which depends on the hardware features of the receiver. In order to maximize the harvested energy, we design the energy beamforming policy as $\mathbf{B}_k = \frac{\mathbf{H}_{k,n}}{\|\mathbf{H}_{k,n}\|}$.

During the data transmission, the received signals at InR and eavesdropper are, respectively, given by,

$$\begin{aligned} \mathbf{y}_{k,n} &= \mathbf{H}_{k,n}\mathbf{x}_{k,n} + \sum_{u\in k}^{U_n} \mathbf{H}_{u,n}\mathbf{x}_{u,n} + \mathbf{n}_{k,n}, \\ \mathbf{y}_{k,n,E} &= \mathbf{G}_{k,n,E}\mathbf{x}_{k,n} + \sum_{u\in k}^{U_n} \mathbf{G}_{u,n,E}\mathbf{x}_{u,n} + \mathbf{n}_{k,n,E}, \end{aligned} \quad (2)$$

where $\mathbf{H}_{k,n} \in \mathbb{C}^{N_T \times N_R}$ and $\mathbf{G}_{k,n,E} \in \mathbb{C}^{N_E \times N_R}$ are the channel coefficient matrices including the path loss effect between the InT k and InR, and between the InT k and eavesdropper, respectively. $\mathbf{x}_{k,n} \in \mathbb{C}^{N_R \times 1}$ denotes the transmitted signal of InT. $\mathbf{n}_{k,n} \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{n}_{k,n,E} \in \mathbb{C}^{N_E \times 1}$ are the additive white Gaussian noise (AWGN) at InR and the eavesdropper, respectively. The noises follow the distribution $\mathcal{CN}(0, \sigma^2 \mathbf{I}_{N_T})$ and $\mathcal{CN}(0, \sigma^2 \mathbf{I}_{N_E})$, respectively. To prevent the eavesdropper overhearing the information data, the InT can add artificial noise to the transmission signal in the following way:

$$\mathbf{x}_{k,n} = \mathbf{b}_{k,n} u_{k,n} + \mathbf{V}_{k,n}\mathbf{v}_{k,n}, \quad (3)$$

where $u_{k,n}$ is the information bearing signal. Precoding is adopted to improve the system throughput. $\mathbf{b}_{k,n} \in \mathbb{C}^{N_T \times 1}$ is the precoding vector. $\mathbf{v}_{k,n} \in \mathbb{C}^{(N_R-1)\times 1}$ is artificial noise vector whose elements are independent and identically distributed (i.i.d.) complex Gaussian random variables with variance $\sigma_{k,n,v}^2$. Without loss of generality, we define the orthogonal basis $\mathbf{V}_{k,n} \in \mathbb{C}^{N_R \times (N_R-1)}$ for the null space of $\mathbf{H}_{k,n}$ such that $\mathbf{H}_{k,n}\mathbf{V}_{k,n}\mathbf{v}_{k,n} = 0$ and $\mathbf{V}_{k,n}^\dagger \mathbf{V}_{k,n} = \mathbf{I}_{N_R-1}$ where $\mathbf{I}_{N_R-1}$ is a $(N_R-1)\times(N_R-1)$ identity matrix, i.e., artificial noise will do nothing for the desired receiver. We denote $p_{k,n}$ as the transmit power of InT k on subchannel n, where we have $p_{k,n} = \frac{E_{k,n}}{(1-\tau)T}$, and $\beta_{k,n}$ as the fraction of transmit power. Then, choosing $\mathbf{b}_{k,n} = \beta_{k,n} p_{k,n} \mathbf{H}_{k,n}^\dagger / \|\mathbf{H}_{k,n}\|$, such that $u_{k,n}$ lies in the range space of $\mathbf{H}_{k,n}$. As can be seen, the transmitted signal consists of two parts. One is the information bearing signal and the other one the artificial noise. Correspondingly, One important design parameter is the ratio of power allocated to the information bearing signal and the artificial noise. The power of artificial noise vectors can be given by [9],

$$\sigma_{k,n,v}^2 = \frac{(1-\beta_{k,n})p_{k,n}}{N_R - 1}. \quad (4)$$

B. Secure Capacity

We adopt the descending order of channel gains as the decoding order, in order to enhance the throughput of weak-channel users and enhance user fairness [1]. We sort all U_n InTs on each subchannel n in descending order of channel gains, $|\mathbf{H}_{1,n}| \geq |\mathbf{H}_{2,n}| \geq ... \geq |\mathbf{H}_{U_n,n}|$. The 1st user (the strongest user) is detected and decoded first by treating all the other users' signals as noise. For the U_nth user (the weakest user), the BS successively decodes and removes all the interference of strong users from 1 to $U_n - 1$, before decoding the signals of the weakest user. Correspondingly, the achievable uplink data rate of k on subchannel n, $C_{k,n}$, can be expressed as $C_{k,n} = WT(1-\tau)\log_2(1+\gamma_{k,n})$, where $\gamma_{k,n}$ is the uplink SINR of k . It can be given as

$$\gamma_{k,n} = \frac{\beta_{k,n} p_{k,n} \|\mathbf{H}_{k,n}\|^2}{\sigma^2 + \sum_{u=k+1}^{U_n} \beta_{u,n} p_{u,n} \|\mathbf{H}_{u,n}\|^2}, \quad (5)$$

where σ^2 is the noise variance. $p_{k,n}$ is the transmit power of k on subchannel n. In this work, all the harvesting energy can be used for transmitting data. The data rate of the eavesdropper of $C_{k,n,E}$ is considered as a random variable, which can be given as $C_{k,n,E} = WT(1-\tau)\log_2(1+\Gamma_{k,n,E})$, where $\Gamma_{k,n,E}$ is the SINR. We also assume that the eavesdropper is much closer to the InT than the desired InR, the eavesdropper noise is negligible.Based on (2), (3) and (4) it can be given as $\Gamma_{k,n,E} = \frac{N_R-1}{1-\beta_{k,n}} \tilde{\mathbf{g}}^\dagger \left(\widetilde{\mathbf{G}}\widetilde{\mathbf{G}}^\dagger\right)^{-1} \tilde{\mathbf{g}}$, where $\tilde{\mathbf{g}} = \mathbf{G}_{k,n,E}\mathbf{b}_{k,n}$ and $\widetilde{\mathbf{G}} = \mathbf{G}_{k,n,E}\mathbf{V}_{k,n}$. $\mathbf{G}_{k,n,E}$ is the channel co-efficient between k and eavesdropper on subchannel n. A worst-case assumption is adopted here for estimating the data rate of eavesdropper

due to the conservativeness mandated by the security studies. Correspondingly, the secrecy capacity of user k on subchannel n can be expressed as

$$C_{k,n}^{s} = (C_{k,n} - C_{k,n,E})\phi(C_{k,n} > C_{k,n,E}), \tag{6}$$

where $\phi(C_{k,n} > C_{k,n,E}) = \begin{cases} 1, & \text{if } C_{k,n} > C_{k,n,E}; \\ 0, & \text{otherwise.} \end{cases}$

III. Problem Formulation

In this Section, we present the formulation of EE problem and also explain the practical constraints. First, to facilitate the presentation of EE formulation, we define a subchannel allocation indicator $\omega_{k,n}$ as follow,

$$\omega_{k,n} = \begin{cases} 1, & \text{if subchannel } n \text{ is allocated to the user } k; \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Next, to formulate the optimization problem, we utilize the definition the EE of the considered system in bits/J as follows [10]: $\mathbf{\Sigma}(\mathbf{P}, \tau, \boldsymbol{\omega}) = \frac{\mathcal{U}(\mathbf{P},\tau,\boldsymbol{\omega})}{\mathcal{P}(\mathbf{P},\tau,\boldsymbol{\omega})}$, where $\mathcal{P}(\mathbf{P}, \tau)$ is the total energy consumption in a time block T and it can be expressed as

$$\mathcal{P}(\mathbf{P}, \tau) = \sum_{n=1}^{N} \tau \nu T P_n + P_c T, \tag{8}$$

where $\mathbf{P}$ is a collection of all power elements, and P_c is the static power consumption, such as the power consumption on baseband and RF chain for antenna. ν is the factor standing for the nonlinear power amplifier effect. We consider $\mathcal{P}(\mathbf{P}, \tau, \boldsymbol{\omega})$ is interchangeable with $\mathcal{P}(\mathbf{P}, \tau)$, and

$$\mathcal{U}(\mathbf{P}, \tau, \boldsymbol{\omega}) = \sum_{k=1}^{K} \sum_{n=1}^{N} \omega_{k,n} R_{k,n} \mathbf{Pr}\{R_{k,n} < C_{k,n} - C_{k,n,E} | \Delta\}, \tag{9}$$

where Δ is the CSI of user k on subchannel n. To this end, we jointly optimize duration τ, allocation indicators $\boldsymbol{\omega}$, and power allocation $\mathbf{P} = \{P_1, \ldots, P_n, \ldots, P_N\}$.

The optimization problem is formulated in **P1**. Our goal is to maximize the system EE under a set of practical constraints. **C1** is the QoS metric for communication security, where ε denotes the maximum tolerable secrecy outage probability. **C2** and **C3** impose limitations on the power consumption and ensure the feasibility of power allocation solutions. Specifically in **C2**, total transmit power for WPT at EnT is no larger than a maximum power limit $P_{b,max}$. In **C3**, we use $\frac{\vartheta \tau P_n \|\mathbf{H}_{k,n}\|^2}{(1-\tau)}$ to represent the power value of UE k on subchannel n, i.e., $p_{k,n}$. Each user's transmit power for uplink data transmission cannot exceed its maximum power limit $P_{u,max}$. In **C4**, R_{min} is the minimum system secrecy rate requirement, and a balance between EE and secrecy outage capacity can be achieved by varying R_{min}. Constraint **C5** indicates that the maximum number of allocated users on each subchannel is up to L. Constraints **C6** to **C7** are the boundary for optimization variables. The formulated problem is with a non-convex structure. The objective function in a fractional program is a ratio of two functions of the optimization variables. In order to make the problem solvable, we transform the objective function and approximate the transformed objective function.

$$\mathbf{P1:} \quad \max_{\mathbf{P},\tau,\boldsymbol{\omega}} \mathbf{\Sigma}(\mathbf{P}, \tau, \boldsymbol{\omega}),$$

$$\mathbf{s.t.}$$

$$\mathbf{C1}: \quad \mathbf{Pr}\{R_{k,n} \geqslant C_{k,n} - C_{k,n,E} | \Delta\} \leqslant \varepsilon, \forall k \in \mathcal{K}, \forall n \in \mathcal{N}$$

$$\mathbf{C2}: \quad \sum_{n=1}^{N} P_n \leqslant P_{b,max},$$

$$\mathbf{C3}: \quad \sum_{n=1}^{N} \frac{\vartheta \tau P_n \|\mathbf{H}_{k,n}\|^2}{(1-\tau)} \leq P_{u,max}, \ \forall k \in \mathcal{K}$$

$$\mathbf{C4}: \quad \sum_{n=1}^{N} R_{k,n} \geqslant R_{min}, \ \forall k \in \mathcal{K}$$

$$\mathbf{C5}: \quad \sum_{k=1}^{K} \omega_{k,n} \leq L, \ \forall n \in \mathcal{N}$$

$$\mathbf{C6}: \quad \omega_{k,n} \in \{0, 1\}, \text{ and } P_n \geq 0,$$

$$\mathbf{C7}: \quad 0 < \tau \leq 1,$$

IV. Proposed Resource Allocation Scheme

A. Transformation of the Optimization Problem

We apply the solution from the fractional programming and transform the objective function and approximate the transformed objective function in order to simplify the problem. We can apply the nonlinear fractional programming method to solve the formulated problem [11]. As can be found in the Sec. IV-B, it can be found that $\mathbf{\Sigma}(\mathbf{P}, \tau, \boldsymbol{\omega})$ can be transformed to a quasi-concave function over the decision variable, then we define the maximum energy efficiency q^* of the considered system and the following theorem can be arrived.

Theorem 1. *The maximum EE q^* can be achieved if and only if*

$$\mathbf{U}(\boldsymbol{P}^*, \tau^*, \boldsymbol{\omega}^*) - q^* \mathcal{P}(\boldsymbol{P}^*, \tau^*, \boldsymbol{\omega}^*) = 0, \tag{10}$$

The proof is similar to the one in [10]. To find the optimal q^*, the iterative algorithm with guaranteed convergence in [11] can be applied. During each iteration, we need to solve the following problem for a given q,

$$\begin{aligned} \mathbf{P2:} \quad & \max_{\mathbf{P},\tau,\boldsymbol{\omega}} \mathbf{U}(\mathbf{P}, \tau, \boldsymbol{\omega}) - q\mathcal{P}(\mathbf{P}, \tau, \boldsymbol{\omega}), \\ & \mathbf{s.t.} \ \mathbf{C1} - \mathbf{C7}. \end{aligned} \tag{11}$$

In order to address the formulated problem, next, we aim at obtaining the secrecy capacity $R_{k,n}$. Correspondingly, the following conclusion can be achieved. Assuming the channel between the InT and eavesdropper is Rayleigh fading, the equivalent secure data rate for InT k is given by

$$R_{k,n} = WT(1-\tau)\Big[\log_2(1+\gamma_{k,n}) - \log_2\left(\frac{\beta_{k,n}^* \Omega_E^{1/2}}{1-\beta_{k,n}^*}\right)\Big]^+, \tag{12}$$

where $\Omega_E = (N_R - 1)F_{z_h}^{-1}(\varepsilon)$, $\beta_{k,n}^* = \frac{1}{\sqrt{2\Omega_E}}$. We also assume that $\gamma \gg 1$. $F_{z_h}^{-1}(\varepsilon)$ is the inverse function of

$F_{z_h}(z) = \varepsilon$, and ε denotes the maximum tolerable secrecy outage in $\mathbf{C1}$. $F_{z_h}(z)$ is given by

$$F_{z_h}(z) = \frac{\sum_{n=0}^{N_E-1} \binom{N_R-1}{n} 2z^n}{(1+z)^{N_R-1}} - \frac{\sum_{n=0}^{N_E-1}\sum_{m=0}^{N_E-1} \binom{N_R-1}{n}\binom{N_T-1}{m} z^{m+n}}{(1+z)^{2N_R-2}}. \quad (13)$$

From the above, it can be found that the SINR from the InT to the eavesdropper becomes a constant value at high SNR and it is independent of the decision variables, which simplifies the derivation of the resource allocation scheme. With the above analysis, in the following, we can address the transformed optimization problems.

B. Proposed Algorithmic Solution

The transformed problem **P2** is still with a non-convex structure. Tackling the mixed non-convex and combinatorial optimization problem requires a prohibitively high complexity. In the next, we firstly relax the problem and decompose the whole optimization process, then we design an iterative search method with guaranteed convergence, and solve the problem to the optimum at each iteration. The proposed algorithmic solution is based on the following analytical results. Firstly, one can observe that from (12), the entity $\log_2\left(\frac{\beta^*_{k,n}\Omega_E^{1/2}}{1-\beta^*_{k,n}}\right)$ in $R_{k,n}$ is approximately a constant. Constraint $\mathbf{C1}$ can be absorbed into objective function in **P2** or **P1**, without loss optimality. Hence, we can rewritten $R_{k,n}$ as $WT(1-\tau)\Big[\log_2(1+\gamma_{k,n}) - \tilde{V}_{k,n}\Big]^+$, where $\tilde{V}_{k,n} = \log_2\left(\frac{\beta^*_{k,n}\Omega_E^{1/2}}{1-\beta^*_{k,n}}\right)$ is seen as a parameter. Secondly, if we consider the rate function in uplink NOMA, the summation of $\log_2(1+\gamma_{k,n})$ over users on each subchannel is $\sum_{k=1}^{K}\log_2(1+\gamma_{k,n}) = \log_2\frac{\sum_{k=1}^{K}\beta_{k,n}p_{k,n}\|\mathbf{H}_{k,n}\|^2}{\sigma^2}$. Based on the above two observations, for any given τ and q, if $\mathbf{C5}$ is temporarily removed or relaxed from **P2**, also replacing all entities $\log_2\left(\frac{\beta^*_{k,n}\Omega_E^{1/2}}{1-\beta^*_{k,n}}\right)$ and $\log_2(1+\gamma_{k,n})$ by the derived new forms, we formulate a relaxed version of **P2** in **P3**.

$$\textbf{P3:} \max_{\mathbf{P}\succeq 0} WT(1-\tau)\sum_{n=1}^{N}\log_2\left(\frac{\sum_{k=1}^{K}\alpha_{k,n}P_n}{\sigma^2}\right) - \sum_{k=1}^{K}\sum_{n=1}^{N}\tilde{V}_{k,n} - q\left(\sum_{n=1}^{N}\tau\nu P_n + P_cT\right),$$

$$\text{s.t. } \mathbf{C2},\ \mathbf{C3},$$

$$\mathbf{C4}: \sum_{n=1}^{N} WT(1-\tau)\log_2\left(1+\frac{\alpha_{k,n}P_n}{\sigma^2+\sum_{u=k+1}^{K}\alpha_{u,n}P_n}\right) - \tilde{V}_{k,n} \geqslant R_{min},\ \forall k\in\mathcal{K}$$

We next show **P3** can be solved efficiently. In P3, $\alpha_{k,n} = \beta_{k,n}\vartheta\tau/(1-\tau)\|\mathbf{H}_{k,n}\|^2\|\mathbf{H}_{k,n}\|^2$, and $WT(1-\tau)\log_2(1+\frac{\alpha_{k,n}P_n}{\sigma^2+\sum_{u=k+1}^{K}\alpha_{u,n}P_n}) - \tilde{V}_{k,n} = R_{k,n}$ in $\mathbf{C4}$. Only power is the optimization variable in **P3**. For the objective function, one can observe its concavity. Constraints $\mathbf{C2}$ and $\mathbf{C3}$ are linear. For $\mathbf{C4}$, we derive the second derivative for function $f(P_n) = \log_2(1+\frac{\alpha_{k,n}P_n}{\sigma^2+\sum_{u=k+1}^{K}\alpha_{u,n}P_n})$. According to the fact that $f''(P_n) < 0$, we therefore conclude the convexity of **P3**.

Algorithm 1 Iterative Algorithm for Solving **P1**

1: **Initialize**: tolerance δ, $Converge$ = false, $Violate$ = false, and $q = 0$;
2: **while** $Converge$ = false **do**
3: **Bisection search** for τ **do**
4: Solve **P3** for current q and τ
5: Obtain optimal power solution $\mathbf{P}$ for **P3**
6: **until** Maximum EE under the current q is achieved at τ' and $\mathbf{P}'$
7: Convert $\mathbf{P}'$ to its corresponding channel indicators $\boldsymbol{\omega}'$
8: **if** ($\mathbf{C5}$ is violated in $\boldsymbol{\omega}'$ and $\mathbf{P}'$) **then**
9: $Violate$ = true
10: **if** $\mathcal{U}(\mathbf{P}',\tau',\boldsymbol{\omega}') - q\mathcal{P}(\mathbf{P}',\tau',\boldsymbol{\omega}') \leq \delta$ **then**
11: $Converge$ = true
12: **return** $\{\mathbf{P}^*,\tau^*,\boldsymbol{\omega}^*\} = \{\mathbf{P}',\tau',\boldsymbol{\omega}'\}$ and update q by (10)
13: **else**
14: $Converge$ = false
15: Update $q = \frac{\mathcal{U}(\mathbf{P}',\tau',\boldsymbol{\omega}')}{\mathcal{P}(\mathbf{P}',\tau',\boldsymbol{\omega}')}$
16: **if** $Violate$ = false **then**
17: **Output 1:** Optimal solution $\{\mathbf{P}^*,\tau^*,\boldsymbol{\omega}^*\}$ for **P1**
18: **else**
19: For τ' and q up to date, convert $\mathbf{P}',\boldsymbol{\omega}'$ to a feasible solution $\bar{\mathbf{P}},\bar{\boldsymbol{\omega}}$ for **P1**
20: **Output 2:** Suboptimal solution $\bar{\mathbf{P}},\bar{\boldsymbol{\omega}}$ for **P1**

The global optimum of a convex problem, e.g., **P3**, can be obtained efficiently by either using standard convex optimization tools. Towards the optimum of **P2**, two aspects can be considered from **P3**. First, given the same q, if the optimal solution in **P3** does not violate $\mathbf{C5}$, it is also optimal for **P2**. On the other side, even if $\mathbf{C5}$ is violated, the similar structure in both problems could lead to high correlation between optimal solutions in **P2** and **P3**, namely, the optimal decisions in **P3** would also be favorable in **P2**. This motivates us to propose an iterative searching scheme in Algorithm 1 to solve the original problem **P1**. Algorithm 1 updates q iteratively, and for each scanned q, the algorithm finds τ by applying bisection search in Line 3 to 6. In each iteration of bisection search, a convex problem **P3** is efficiently solved in Line 4 when τ and q have been updated. The majority of frictional programming is integrated in Line 10 to 17, to decide whether the optimal q is achieved or update suboptimal q in Line 15. According to the proof of [11], the convergence of the proposed algorithm is guaranteed.

V. Performance Evaluation

In the simulations, we consider one energy transmitter/information receiver and multiple users (EHRs/InTs) and the distance between the EnT and users are about 200m. The bandwidth is 3 MHz. As for wireless power transfer, we assume that the energy conversion efficiency of WPT is $\vartheta = 0.5$. A distance-depended path loss model is considered.

To evaluate the performance of proposed scheme (P-NOMA), we have implemented a previous NOMA power and channel allocation scheme called "fractional transmit power control" (FTPC) and an OFDMA scheme with FTPC (OFDMA) [1], [3]. We also compare our proposed scheme with equal transmit power allocation scheme (ETPA) and equal time allocation scheme (ETTA). In ETPA, NOMA system is considered and the transmit power on each subchannel is equal while the other schemes are the same as the proposed one. In ETTA, the proposed power allocation and subchannel allocation are used while overall time slot is divided equally for data transmission and power delivery.

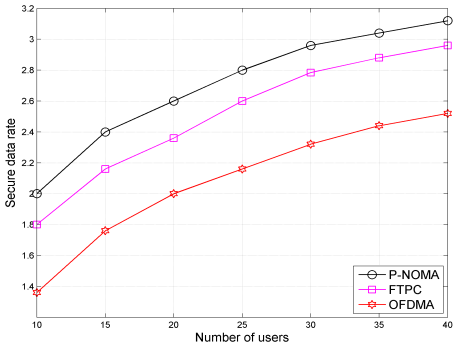

Figure 1. Secure data rate versus number of users/InTs in the system.

Fig. 1 shows the secure data rate (bps/Hz) versus the number of users. We also compare the performance of the P-NOMA with that of the FTPC and OFDMA to show the advantages of our proposed scheme. It can be observed that the secure data rate increases when the number of users grows. As the number of users becomes larger, the secure data rate continues to increment, while the rate of growth becomes slower. From this figure, the proposed resource allocation scheme achieves 10% better performance than the FTPC when the number of users is 25, and is about 50% better than that of OFDMA.

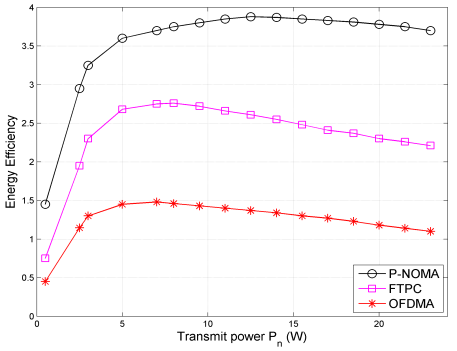

Figure 2. Energy efficiency versus transmit power of the EnT.

Fig. 2 plots the EE by changing the transmit power P_n and allocated time slot τ. The performance of the proposed scheme with optimal time allocation (P-NOMA) is compared with the one of OFDMA with optimal time allocation, and the one of the proposed scheme with equal time allocation (ETTA), e.g. $\tau = 1/2T$. By the comparing these three curves, we can observe that with the increase of transmit power, the EE of the system first ascends and then descends. Fig. 2 shows that the transmit power has an optimal value, which confirms the advantages and necessity of power allocation scheme. Moreover, it can be seen that our proposed time allocation scheme can obtain additional EE gain when comparing with the equal time allocation scheme. Last but not the least, we can find that the EE of our proposed scheme is the highest among all three, which shows the advantages of our proposed algorithms over the traditional schemes.

VI. Conclusion

We have investigated secure-rate and energy-efficient resource allocation problem for NOMA systems empowered by the wireless power transfer. The objective is to obtain secure and energy-efficient transmission among multiple users by investigating time, power and subchannel allocation schemes. We have proposed an iterative algorithm with guaranteed convergence to deliver a competitive suboptimal solution. Performance evaluations have demonstrated the effectiveness of the proposed algorithm over other resource allocation schemes in NOMA or OFDMA system.

VII. Acknowledgments

The work has been supported by the Luxembourg National Research Fund (FNR) CORE project ROSETTA (C17/IS/11632107), the FNR bilateral projects LARGOS and INWIPNET, in part by the Fundamental Research Fund for the Central Universities under Grant 20199176534, China.

References

[1] L. Dai, B. Wang, Y. Yuan, S. Han, C. l. I and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74-81, Sep. 2015.

[2] L. Lei, D. Yuan, and P. Värbrand, "On power minimization for non-orthogonal multiple access (NOMA)," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2458-2461, Dec. 2016.

[3] L. Lei, D. Yuan, C.-K. Ho, and S. Sun, "Power and channel allocation for non-orthogonal multiple access in 5G systems: tractability and computation" *IEEE Transactions on Wireless Communications*, vol. PP, no. 99, pp. 1-1, 2016.

[4] D. K. Nguyen, D. N. Jayakody, S. Chatzinotas, J. Thompson, J. Li, "Wireless Energy Harvesting Assisted Two-Way Cognitive Relay Networks: Protocol Design and Performance Analysis," in IEEE Access, pre-print. 2017.

[5] N. Jayakody, S. Chatzinotas, J. Thompson, and S. Durrani, "Wireless Harvesting for Future Wireless Communications," Springer, ISBN: 978-3-319-56669-6, 2017.

[6] Y. Zhang, H. M. Wang, Q. Yang and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Communications Letters*, vol. 20, no. 5, pp. 930-933, May 2016.

[7] B. He, A. Liu, N. Yang and V. K. N. Lau, "On the Design of Secure Non-Orthogonal Multiple Access Systems," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2196-2206, Oct. 2017.

[8] R. Zhang and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," in *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 1989-2001, May 2013.

[9] X. Zhou, and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal rower Allocation," *IEEE Transactions on Vehicular Technology*, vol 59, no. 8, pp. 3831-3842, Jul. 2010.

[10] Z. Chang, J. Gong, T. Ristaniemi and Z. Niu, "Energy efficient resource allocation and user scheduling for collaborative mobile clouds with hybrid receivers," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9834-9846, Dec. 2016.

[11] W. Dinkelbach, "On nonlinear fractional programming," *Management Science*, vol. 13, no. 7, pp. 492-498, Mar. 1967.