Secure Energy Efficiency for NOMA based Cognitive Radio Networks with Nonlinear Energy Harvesting

Dawei Wang, Member, IEEE, and Shaoyang Men, Member, IEEE

Abstract—In order to improve the spectrum efficiency and secrecy energy efficiency, in this paper, we propose a non-orthogonal multiple access (NOMA) based secure scheme for cognitive radio networks. In the proposed scheme, the secondary users harvest energy from the radio-frequency signals to securely transmit the secondary privacy information with the NOMA technique. Unlike the conventional ideal linear energy harvesting, we employ the practical nonlinear energy harvesting model for energy harvesting. To implement the proposed scheme, the energy transmitter first broadcasts radio-frequency signals to power the secondary users. Then, the secondary users employ the NOMA technique to transmit the uplink privacy information which is threatened by the eavesdropper. Considering two scenarios: two secondary users and more than two secondary users, we first provide comprehensive analysis of the secondary secrecy performances, and derive the closed-form expressions of the secrecy outage probability for both scenarios. Following the above analysis, we develop the optimization problems to optimally allocate the time slot and the secondary transmit power such that the minimum secrecy energy efficiency is maximized under constraints of the transmission security and reliability requirements. A two stages algorithm is proposed to efficiently solve the above optimization problems. Numerical results are presented to verify the analysis in terms of the secrecy rate and secrecy energy efficiency.

Index Terms—Nonlinear energy harvesting, NOMA, Resource allocation, Security.

I. Introduction

Cognitive radio is a promising technique to improve the spectrum efficiency by allocating the secondary users to dynamically access the licensed spectrum [1]–[3]. The underlay and/or overlay spectrum sharing strategies are widely implemented in the current researches about the cognitive radio networks. For the overlay strategy, the secondary users detect the underutilized licensed spectrum to access which can avoid collision with the primary transmission [4]–[6]. For the underlay strategy, the secondary network shares the licensed spectrum with the primary users by controlling the interfere to the primary receivers under a threshold [7]–[9]. Besides cognitive radio technique, non-orthogonal multiple access (NOMA) technique can further improve the spectrum efficiency by allocating multiple users to access the same frequency with different transmit power [10]–[12]. The successive interference cancellation (SIC) is employed at the receiver to distinguish the different signals [12]. Taking advantages of both the cognitive radio and NOMA techniques, the NOMA based cognitive radio networks will not only improve the spectrum efficiency but also serve more secondary users, which is a promising technique for the 5th generation mobile networks [13].

The limited energy supply of the secondary users, such as it is hard to replace the battery and/or there is no power line, limits the secondary performance improvement. To address this problem, energy harvesting technique is proposed to utilize the energy from the surrounding environments. Radio frequency (RF) energy harvesting [14], which harvests the energy from the radio-frequency signals, can provide flexible, sustainable and stable energy supply and has been widely studied in cognitive radio networks [15]–[19]. In [16], [17], the secondary users dynamically decided to sense the primary spectrum or harvest the primary RF energy for battery charging. The authors in [18] proposed an optimal channel selection method to improve the secondary throughput by utilizing the harvested RF energy. The RF energy harvesting was also investigated in cognitive radio sensor networks in [19]. In all the above works, the RF energy harvesting model is ideal linear. However, this model cannot reflect the nonlinear behaviors in the practical energy harvesting circuits [20]–[22]. Therefore, the authors in [20]–[22] proposed the nonlinear RF energy harvesting model and investigated the secondary performance. In addition, the authors in [23] and [24] had studied the optimal resource allocation to maximize the sum information rate or the sum harvested energy of the nonlinear energy harvesting model. Besides the above works, the nonlinear energy harvesting in cognitive radio networks, especially for the NOMA based cognitive radio network, has not been well studied.

It is worth pointing out that the information security is also not concerned in the cognitive radio networks with the nonlinear RF energy harvesting. Due to open spectrum sharing nature, the cognitive radio networks are vulnerable to be eavesdropped since the eavesdropper can pretend to be a secondary user [25]–[27]. In [28], a beamforming scheme was designed to protect both the primary and
secondary privacy information. The authors in [29] studied the secondary secrecy outage probability from Poisson distributed eavesdroppers. In [30], the artificial noise was beamformed to interference the eavesdropper and protect the secondary information. Considering the limited energy supply, the authors in [31] investigated the security and reliability tradeoff by considering the interference to the primary system and the secondary residual harvested energy. In [32], the secondary system harvested the primary RF energy for the secondary secure transmission. In [33], [34], the optimal beamforming schemes were designed to protect the secondary privacy information and power the energy harvesting users. The artificial noise assisted secondary secure transmission was investigated in [35] with energy harvesting. To further improve the spectrum efficiency, the authors in [36] firstly studied the NOMA based secure transmission with nonlinear power harvesting for the secondary downlink transmission. The NOMA based cognitive uplink secure transmission with nonlinear energy harvesting has yet studied which is investigated in this paper.

In this paper, we propose a NOMA based secure transmission scheme in cognitive radio networks to improve the secrecy energy efficiency and spectrum efficiency with nonlinear energy harvesting. In order to implemented the proposed scheme, each time slot is divided into two mini-time slots. In the first mini-time slot, the energy transmitter broadcasts energy signals to power the secondary users. Adopting the practical nonlinear energy harvesting model, the secondary users store the harvested RF energy. In the second mini-time slot, the secondary users employ the NOMA technique to transmit the uplink privacy information, and the secondary receiver utilizes SIC to decode these secondary signals which is eavesdropped by the eavesdropper. For the proposed scheme, we first consider the two secondary users scenario, and we then extend this work to the more than two secondary users scenario. For both scenarios, we provide comprehensive analysis of the secrecy performances, and derive the closed-form expressions of the secrecy outage probability. Following the above results, we develop the optimization problems to allocate the time slot and the transmit power such that the secrecy energy efficiency is maximized under constraints of the transmission security and reliability requirements. A two stages algorithm is proposed to solve the above optimization problems. Numerical results are presented to verify the analysis in terms of the secrecy rate and secrecy energy efficiency. Our contributions are summarized as follows:

- We consider the NOMA based secure uplink transmission in cognitive radio networks with the practical nonlinear energy harvesting. The NOMA technique allow the secondary networks to service multiple secondary users and the nonlinear energy harvesting model can accurately capture the practical energy harvesting process. To the authors' best knowledge, this is the first work that considers the NOMA based cognitive secure uplink transmission with nonlinear energy harvesting.

- We derive the closed-form expressions of the secrecy outage probability. Under the constraint of the transmission security and reliability, we optimally allocate the time slot and transmit power such that the minimum secrecy energy efficiency is maximized. In addition, we develop a two stages algorithm to solve this optimization problem.

- Simulation results show the performance of the proposed scheme in terms of the secrecy rate and secrecy energy efficiency, which slightly lower than the linear energy harvesting model.

The rest of this paper is organized as follows. Section II describes the NOMA based cognitive radio networks. In Section III, we consider the scenario of two secondary users and analyze the secondary secure performance. In addition, we optimally allocate the time slot and transmit power such that the minimum secrecy energy efficiency is maximized. Section IV extends our works to the scenario of more than two secondary users. Similarly, we analyze the secrecy performance and optimally allocate the time slot and transmit power to maximize the minimum secrecy energy efficiency. We conduct extensive simulations in Section V, and Section VI concludes the paper.

II. System Model

We consider a cognitive radio network underlaying the primary network as shown in Fig. 1, where the secondary network shares the same licensed spectrum with the primary network by controlling the interference to primary receivers. The primary network has a transmitter (PT) and a receiver (PR). The secondary network has one secondary access point (AP) to receive the uplink information from multiple secondary transmitters (ST) that are powered by an energy transmitter (ET). In this paper, we first consider two STs (ST₁ and ST₂) scenario, and then we extend our work to M STs scenario (where the
ith ST is denoted as ST$_i$). In addition, there is an passive eavesdropper that threatens the secondary information security. In each time slot, ET first transfers energy to power all STs, and then, STs utilize the NOMA technique to transmit the privacy signals for AP eavesdropped by EV.

Both the primary and secondary networks experience independent, flat, and block Rayleigh fading, which indicates that the system state will independently vary in different time slots and keep invariance in one time slot [36]. The channels ET $\rightarrow$ ST$_i$, ET $\rightarrow$ AP, SU$_i$ $\rightarrow$ AP, PT $\rightarrow$ AP, ST$_i$ $\rightarrow$ PR, and ET $\rightarrow$ PR are denoted as $h_{ii}$, $h_{ip}$, $h_{ia}$, $h_{pa}$, $h_{ip}$, and $h_{ep}$, respectively. Their channel power gains are denoted $g_{ii}$, $g_{ip}$, $g_{ia}$, $g_{pa}$, $g_{ip}$, and $g_{ep}$, which follow exponential distribution with parameters $\lambda_{ii}$, $\lambda_{ip}$, $\lambda_{ia}$, $\lambda_{pa}$, $\lambda_{ip}$, and $\lambda_{ep}$, respectively. The primary and secondary channel state information (CSI) can be acquired through channel estimation [29]. For practical consideration, we assume that the wiretap CSI is unavailable and the wiretap channel distribution information (CDI) can be acquired. For simplicity, we assume that all noise variables are complex Gaussian random variables with zero mean and variance $N_0$ [37]–[40]. The transmit power of PT and ET are denoted as $p_p$ and $p_t$, respectively.

Each time slot with duration $T$ is divided into two mini-slots as shown in Fig. 2. The first mini-slot is employed for energy transfer and the second mini-slot is utilized for secondary privacy information transmission. In the first mini-slot, each ST harvests the energy signals. Considering the practical energy harvesting process, we adopt the nonlinear energy harvesting model as [35], [36]

$$E_h = P_s \left( \frac{a}{1-e^{ab}} - \frac{1}{1-e^{a/b}} \right),$$

(1)

where $P_s$ is the maximum harvested power; $a$ and $b$ are positive constants related to the circuit specification$^1$; $h$ denotes the channel quality of the energy harvesting channel; $P$ denotes the transmit power of the energy transmitter. After harvesting enough energy, STs adopts the NOMA technique to transmit the privacy information, and AT utilizes the SIC technique to detect the privacy information. In addition, the secondary system utilizes the wiretap coding to encrypt the privacy information, which indicates that the target transmission rate $R_b$ and the target secrecy rate $R_s$ are set and the rate difference between $R_b$ and $R_s$ is the rate redundancy against eavesdropping.

Specifically, in the first mini-slot with duration $aT$, ET broadcasts the power signal to STs with power $p_t \leq \frac{E_h I_{th}}{\tau_2}$ where $I_{th}$ is the maximum interference constraint to the primary network. The received signal at ST$_i$ is given by

$$y_i = \sqrt{p_i}h_{ii}x_e + \sqrt{p_t}h_{ip}x_p + n_i,$$

(2)

where $x_e$ is the energy signal with $\mathbb{E} \{|x_e|^2\} = 1$ and $\mathbb{E} \{\cdot\}$ is the expectation operation; $x_p$ is the primary signal with $\mathbb{E} \{|x_p|^2\} = 1$; $n_i$ is the noise variable. According to the nonlinear energy harvesting model, the harvested energy is derived as

$$E_{hi} = P_s \left( 1 - \frac{e^{ab} + 1}{e^{a/b} + e^{ab}} \right).$$

(3)

By utilizing the harvested power, STs transmit the secondary uplink privacy information with NOMA technique to AP in the second mini-slot with duration $\tau_2 T$, and the received signal at AP is given by

$$y_a = \sum_{i=1}^{M} \sqrt{p_i}h_{ia}x_i + \sqrt{p_p}h_{pa}x_p + n_b,$$

(4)

where $p_i$ is ST$_i$ transmit power; $n_b$ is the received noise at AP. In addition, EV also receives the privacy information as

$$y_e = \sum_{i=1}^{M} \sqrt{p_i}h_{ie}x_i + \sqrt{p_p}h_{pe}x_p + n_e,$$

(5)

where $n_e$ is the noise variable at EV. After receiving the privacy signals, AP and EV decode these signals according to the SIC technique.

In the following, we first study the NOMA based secure transmission for two STs and optimally allocate the time slot and the transmit power. Then, we extend our work to $M (M \geq 3)$ STs scenario.

III. Secure Transmission for NOMA based Wirelessly Powered Cognitive Network with Two STs

In this section, two STs, denoted as ST$_1$ and ST$_2$, are considered for the NOMA based uplink cognitive network. We first analyze the secondary secrecy performance, and then we allocate the transmit power and time slot according to the above analysis.

A. Secondary Secrecy Performance

During the energy harvesting process, the harvested energy for ST$_1$ and ST$_2$ are derived as

$$\begin{align*}
E_{h1} &= P_s \left( 1 - \frac{e^{ab} + 1}{e^{a/b} + e^{ab}} \right), \\
E_{h2} &= P_s \left( 1 - \frac{e^{ab} + 1}{e^{a/b} + e^{ab}} \right).
\end{align*}$$

(6)

Limited by the harvested energy and the primary interference threshold, the transmit power of ST$_1$ and ST$_2$ should satisfy $p_1 \leq \frac{E_{h1}}{\tau_1}$, $p_2 \leq \frac{E_{h2}}{\tau_1}$ and $p_1 g_{1p} + p_2 g_{2p} \leq I_{th}$.
Assuming $g_{1a} \leq g_{2a}$, AP employs SIC to decode the received both ST$_1$ and ST$_2$'s privacy messages. By taking ST$_1$'s message as interference, AP first decodes ST$_2$'s message with rate as

$$R_{2a} = \frac{T}{T} \log_2 \left( 1 + \frac{p_{2g2a}}{p_{g1a} + p_{p8pa} + N_0} \right).$$

(7)

After decoding ST$_2$'s message, AP decodes ST$_1$'s message with rate as

$$R_{1a} = \frac{T}{T} \log_2 \left( 1 + \frac{p_{1g1a}}{p_{p8pa} + N_0} \right).$$

(8)

Similarly, EV also employs SIC to decode the privacy information. Taking ST$_1$'s message as noise, EV first decodes ST$_2$'s message with rate as

$$R_{2e} = \frac{T}{T} \log_2 \left( 1 + \frac{p_{2g2e}}{p_{g1e} + p_{p8pe} + N_0} \right).$$

(9)

After decoding ST$_2$'s message, EV decodes ST$_1$'s message with rate as

$$R_{1e} = \frac{T}{T} \log_2 \left( 1 + \frac{p_{1g1e}}{p_{p8pe} + N_0} \right).$$

(10)

Therefore, the secrecy rates for ST$_1$ and ST$_2$ are respectively given by

$$R_{1s} = (R_{1a} - R_{1e})^+ = \left( \frac{T}{T} \log_2 \left( 1 + \frac{p_{1g1a}}{p_{p8pa} + N_0} \right) - \frac{T}{T} \log_2 \left( 1 + \frac{p_{1g1e}}{p_{p8pe} + N_0} \right) \right)^+$$

(11)

and

$$R_{2s} = (R_{2a} - R_{2e})^+ = \left( \frac{T}{T} \log_2 \left( 1 + \frac{p_{2g2a}}{p_{g1a} + p_{p8pa} + N_0} \right) - \frac{T}{T} \log_2 \left( 1 + \frac{p_{2g2e}}{p_{g1e} + p_{p8pe} + N_0} \right) \right)^+$$

(12)

where $(a)^+ = \max(0, a)$.

Since EV is a passive eavesdropper, we cannot acquire the wiretap CSI. Therefore, we utilize the secrecy outage probability to evaluate the secrecy performance. According to the wiretap coding, when $R_{1e} \leq (R_b - R_s)$, ST$_1$’s privacy information is eavesdropped; when $R_{2e} \leq (R_b - R_s)$, ST$_2$’s privacy information is eavesdropped. Therefore, the secrecy outage probability for ST$_1$ is derived as

$$P_{1,so} = \Pr(R_{1e} \geq (R_b - R_s))$$

$$= \Pr \left( \frac{T}{T} \log_2 \left( 1 + \frac{p_{1g1e}}{p_{g1e} + p_{p8pe} + N_0} \right) \geq (R_b - R_s) \right)$$

$$= \int_0^\infty \exp \left( - \left( \frac{2T}{T} (R_b - R_s) - 1 \right) p_{p8pe} (y) \right) df_{pe} (y) dy$$

$$= \frac{p_{1g1e}}{p_{1g1e} + p_{p9pe}} \exp \left( - \left( \frac{2T}{T} (R_b - R_s) - 1 \right) N_0 \right)$$

(13)

where $f_{pe}$ denotes the probability density function (PDF) of $g_{pe}$. The secrecy outage probability for ST$_2$ is derived as

$$P_{2,so} = \Pr(R_{2e} \geq (R_b - R_s))$$

$$= \Pr \left( \frac{T}{T} \log_2 \left( 1 + \frac{p_{2g2e}}{p_{g1e} + p_{p8pe} + N_0} \right) > (R_b - R_s) \right)$$

$$= \int_0^\infty \exp \left( - \left( \frac{2T}{T} (R_b - R_s) - 1 \right) (p_{p8pe} + N_0) \right) \times f_{ge} (x) f_{pe} (y) dx dy$$

$$= \left( \frac{p_{2g2e}}{p_{2g2e} + p_{p9pe}} \right) \times \exp \left( - \left( \frac{2T}{T} (R_b - R_s) - 1 \right) N_0 \right)$$

(14)

In the following, we will optimally allocate the time slot and transmit power to maximize the secrecy energy efficiency according to the above analysis.

B. Transmit Power and Time Slot Allocation

In order to maximize the secrecy energy efficiency, we formulate the optimal problem as

$$\begin{align*}
\textbf{P1} : \max_{T_1, T_2, P_1, P_2} & \left( \frac{R_1 (1 - P_{1,so})}{P_1 + P_c}, \frac{R_2 (1 - P_{2,so})}{P_2 + P_c} \right) \\
\text{s.t.} & R_1 \geq R_b \\
& R_2 \geq R_b \\
& P_1 \leq \frac{E_{h1T_1}}{T_1} \\
& P_2 \leq \frac{E_{h2T_2}}{T_2} \\
& p_{1g1p} + p_{2g2p} \leq I_{th} \\
& P_{1,so} < \xi \\
& P_{2,so} < \xi \\
& T_1 + T_2 = 1
\end{align*}$$

(15a)

where $P_c$ is the is the constant power consumed by the circuit; $\xi$ is the maximum permitted secrecy outage probability. In $\textbf{P1}$, (15a) denotes the maximization of the minimum secrecy energy efficiency of ST$_1$ and ST$_2$; (15b) and (15c) guarantee the successfully decoding of the privacy information; (15d), (15e), and (15f) are the power constraints; (15g) and (15h) are the secrecy outage probability constraints. Since $\textbf{P1}$ is non-convex, we cannot directly acquire the optimal power and time allocation parameters through the traditional convex algorithm. To solve this problem, we propose a two stages algorithm.

1) Given the Time Allocation Parameter $T_1$: Assuming $T_1$ is given, $\textbf{P1}$ can be transformed to the optimal power allocation and power control parameters problem as

$$\begin{align*}
\textbf{P2} : \max_{P_1, P_2} & \left( \frac{R_1 (1 - P_{1,so})}{P_1 + P_c}, \frac{R_2 (1 - P_{2,so})}{P_2 + P_c} \right) \\
\text{s.t.} & P_1 \leq \frac{E_{h1T_1}}{T_1} \\
& P_2 \leq \frac{E_{h2T_2}}{T_2} \\
& p_{1g1p} + p_{2g2p} \leq I_{th} \\
& P_{1,so} < \xi \\
& P_{2,so} < \xi \\
& T_1 + T_2 = 1
\end{align*}$$

(15a)

which is non-convex, we cannot directly acquire the optimal power and time allocation parameters through the traditional convex algorithm. To solve this problem, we propose a two stages algorithm.
allocation problem as

\[
\textbf{P11} : \max_{p_1, p_2} \left( \frac{R_i (1 - P_{1,so})}{p_1 + p_c}, \frac{R_s (1 - P_{2,so})}{p_2 + p_c} \right)
\]

s.t. \( R_{1a} \geq R_b \),
\( R_{2a} \geq R_b \),
\( p_1 \leq \frac{E_{b1} \tau_1}{T_2} \),
\( p_2 \leq \frac{E_{b2} \tau_1}{T_2} \),
\( P_{1g1p} + P_{2g2p} \leq I_{th} \),
\( P_{1,so} < \xi \),
\( P_{2,so} < \xi \).

For (16b) and (16c), they can be rewritten as

\[
p_1 \geq p_1^{\text{min}} = \frac{\left( \frac{R_i}{T_2} - 1 \right) \left( p_p g_{pa} + N_0 \right)}{g_{1a}}
\]

and

\[
p_2 \geq p_2^{\text{min}} = \frac{\left( \frac{R_s}{T_2} - 1 \right) \left( p_p g_{pa} + N_0 \right)}{g_{2a}}.
\]

For (16f), it can be transformed as \( p_1 \leq \frac{I_{th} - P_{1g1p}}{g_{1p}} \) and \( p_2 \leq \frac{I_{th} - P_{2g2p}}{g_{2p}} \). For (16b), since \( P_{1,so} \) is a monotonically increasing function of \( p_1 \), \( p_1^* \)'s maximum value \( p_1^{\text{opt}} \) satisfies \( P_{1,so}(p_1^{\text{opt}}) = \xi \). Therefore, when \( p_1 \leq p_1^{\text{opt}} \), \( P_{1,so}(p_1) \leq \xi \). Similarly, for (16b), since \( P_{1,so} \) is a monotonically increasing function of \( p_1 \), \( p_2^* \)'s maximum value \( p_2^{\text{opt}} \) that satisfies \( P_{2,so}(p_2^{\text{opt}}) = \xi \). When \( p_2 \leq p_2^{\text{opt}} \), \( P_{2,so}(p_2) \leq \xi \).

According to the above discussion, when \( p_1^{\text{min}} > \min \left( \min \left( \frac{I_{th} - P_{1g1p}}{g_{1p}}, \frac{E_{b1} \tau_1}{T_2} \right), \frac{E_{b1} \tau_1}{T_2} \right) \), there is no optimal \( p_1 \) that satisfies the optimal problem \( \textbf{P11} \); otherwise, when \( p_1^{\text{min}} \leq p_1 \leq \min \left( \min \left( \frac{I_{th} - P_{1g1p}}{g_{1p}}, \frac{E_{b1} \tau_1}{T_2} \right), \frac{E_{b1} \tau_1}{T_2} \right) \), there is an optimal \( p_1 \left( p_1^{\text{min}} \leq \min \left( \min \left( \frac{I_{th} - P_{1g1p}}{g_{1p}}, \frac{E_{b1} \tau_1}{T_2} \right), \frac{E_{b1} \tau_1}{T_2} \right) \right) \) that satisfies the optimal problem \( \textbf{P11} \). Similarly, when \( p_2^{\text{min}} \leq \min \left( \min \left( \frac{I_{th} - P_{2g2p}}{g_{2p}}, \frac{E_{b2} \tau_1}{T_2} \right), \frac{E_{b2} \tau_1}{T_2} \right) \), there is an optimal \( p_2 \left( p_2^{\text{min}} \leq p_2 \leq \min \left( \min \left( \frac{I_{th} - P_{2g2p}}{g_{2p}}, \frac{E_{b2} \tau_1}{T_2} \right), \frac{E_{b2} \tau_1}{T_2} \right) \right) \) that satisfies the optimal problem \( \textbf{P11} \).

\[
\text{IV. Secure Transmission for NOMA based Wirelessly Powered Cognitive Network with } M (M \geq 3) \text{ STs}
\]

In this section, we will study the secure transmission for NOMA based wirelessly powered cognitive network with \( M (M \geq 3) \) STs. Similar with Section III, we first investigate the secrecy performance, and then we will optimally allocate the transmit power and time slot to maximize the minimum secrecy energy efficiency.

A. Secondary Secrecy Performance

In the first mini-slot, \( ST_i \) harvests the energy from the received radio-frequency signal as

\[
E_{hi} = P_s \left( 1 - \frac{e^{ab} + 1}{e^{a(bP_{p,sp} + P_{sp} + N_0)} + e^{ab}} \right).
\]

Utilized the harvested energy, all STs transmit their privacy signals to AP. Assuming \( s_{1a} \leq s_{2a} \leq \cdots \leq s_{Ka} \) and adopting the SIC technique, we can derive the information rates for \( ST_i \) according to (4) as

\[
R_{ia} = \frac{C}{T} \log_2 \left( 1 + \frac{P_{ri} g_{ia}}{\sum_{k=1}^{K} P_k g_{ka} + P_p s_{pa} + N_0} \right), 1 \leq i \leq K - 1
\]

\[
R_{ka} = \frac{C}{T} \log_2 \left( 1 + \frac{P_k g_{ka}}{P_p s_{pa} + N_0} \right), i = K.
\]

Similarly, the eavesdropping rates for EV are

\[
R_{ie} = \frac{C}{T} \log_2 \left( 1 + \frac{P_{ri} g_{ie}}{\sum_{k=1}^{K} P_k g_{ke} + P_p s_{pe} + N_0} \right), 1 \leq i \leq K - 1
\]

\[
R_{ke} = \frac{C}{T} \log_2 \left( 1 + \frac{P_k g_{ke}}{P_p s_{pe} + N_0} \right), i = K.
\]
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2876970, IEEE Access

Therefore, the secrecy rates for ST \( i \leq i \leq K - 1 \) are derived as

\[
P_i = (R_{ia} - R_{ie})^+ \quad (25)
\]

and the secrecy rate for ST \( K \) is

\[
P_K = (R_{ka} - R_{ke})^+ \quad (26)
\]

Since the wiretap CSI is unavailable, we employ the secrecy outage probability to evaluate the secrecy performance. For ST \( i \) \( (1 \leq k \leq K - 1) \), the secrecy outage probability is derived in (27) at the top of the next page. For ST \( K \), the secrecy outage probability is derived as

\[
P_{K,i} = \Pr(R_{ke} \geq (R_b - R_s)) \quad (28)
\]

B. Transmit Power and Time Slot Allocation

To maximize the minimum secrecy energy efficiency, we formulate the optimal problem as

\[
P_2 : \max_{\tau_1, \tau_2, \cdots, \tau_K} \min_{p_1, \cdots, p_K} \left\{ \frac{R_s (1 - P_{i,io})}{p_1 + p_c}, \cdots, \frac{R_s (1 - P_{K,io})}{p_K + p_c} \right\} \quad (29a)
\]

\[
s.t. R_{ia} \geq R_b, i = 1, \cdots, K \quad (29b)
\]

\[
p_i \leq \frac{E_a \tau_i}{\tau_2}, i = 1, \cdots, K \quad (29c)
\]

\[
\sum_{i=1}^K p_i g_{ip} \leq I_{th} \quad (29d)
\]

\[
P_{i,io} < \xi, i = 1, \cdots, K \quad (29e)
\]

\[
\tau_1 + \tau_2 = 1. \quad (29f)
\]

In (29a) denotes the maximization of the minimum secrecy energy efficiency; (29b) denotes the successful decoding constraint; (29c) indicates that the transmit power is limited by the harvested energy; (29d) denotes the primary interference constraint; (29e) is the secondary information security constraint. Since (29a) is also noncoex, we cannot solve this problem through the traditional convex method directly. Therefore, we still adopt the two-stage algorithm to solve this problem.

1) Given the Time Slot Allocation Parameter \( \tau_1 \): Given the time allocation parameter \( \tau_1 \), the optimal problem can be transformed as

\[
P_{21} : \max_{p_1, \cdots, p_K} \min_{\tau_2} \left\{ \frac{R_s (1 - P_{i,i0})}{p_1 + p_c}, \cdots, \frac{R_s (1 - P_{K,i0})}{p_K + p_c} \right\} \quad (30a)
\]

\[
s.t. R_{ia} \geq R_b, i = 1, \cdots, K \quad (30b)
\]

\[
p_i \leq \frac{E_a \tau_1}{\tau_2}, i = 1, \cdots, K \quad (30c)
\]

\[
\sum_{i=1}^K p_i g_{ip} \leq I_{th} \quad (30d)
\]

\[
P_{i,i0} < \xi, i = 1, \cdots, K \quad (30e)
\]
Regarding to the nonlinear energy harvesting model, we addition, the path loss parameter is set to
channel model is utilized to model the wireless channels. In
allocation parameters for the secrecy energy efficiency
For (30d), we can acquire
Since $P_{1,s,o}$ is the monotonic increasing function of $p_i$, we can acquire the maximum $p_i^{\text{max}_2}$ which satisfies $P_{1,s,o}(p_i^{\text{max}_2}) = \xi$. In addition, when $p_i \leq p_i^{\text{max}_2}$, $P_{1,s,o}(p_i) = \xi$. Therefore, the optimal $p_i$ should satisfy $p_i^{\text{min}} \leq p_i \leq \min\{p_i^{\text{max}_1}, p_i^{\text{max}_2}, E_{\text{th}}/p_a\}$.

Set $EE_i = R_s(1-p_{1,s,o})$. Since $EE_i$ is a monotonic decreasing function of $p_i$, the optimal $p_i$ should be

and

The (30b) can be rewritten as

\[
p_i \geq p_i^{\text{min}} = \frac{\left( \sum_{k=i+1}^{K} P_k g_k + p_p g_p + N_0 \right)}{g_K a} \times \left( 2^{\frac{T R_b}{T_2}} - 1 \right), \ 1 \leq i \leq K - 1
\]

and

\[
p_K \geq p_K^{\text{min}_K} = \frac{(2^{\frac{T R_b}{T_2}} - 1)(p_p g_p + N_0)}{g_K a}, i = K.
\]

For (30d), we can acquire

\[
p_i \leq p_i^{\text{max}_1} = \frac{I_{th}}{\sum_{k=1, k \neq i}^{K} P_k g_k}, i = 1, \ldots, K.
\]

\[
p_i^{\text{opt}} = \left( \frac{\sum_{k=i+1}^{K} P_k g_k + p_p g_p + N_0}{g_K a} \times \left( 2^{\frac{T R_b}{T_2}} - 1 \right), \ 1 \leq i \leq K - 1
\]

\[
p_K^{\text{opt}} = \frac{(2^{\frac{T R_b}{T_2}} - 1)(p_p g_p + N_0)}{g_K a}, i = K.
\]

2) The Optimal Time Allocation: Submitted the derived optimal transmit power $p_i^{\text{opt}}$ into $EE_i$, we will acquire the optimal time allocation parameter through the one-dimensional search to maximize the following optimal problem

\[
P22: \max_{\tau_1} \ \\frac{R_s (1-p_{1,s,o})}{p_1 + p_c}, \ldots, \frac{R_s (1-p_{K,s,o})}{p_K + p_c}
\]

\[\text{s.t.} \ \tau_1 + \tau_2 = 1.
\]

Then, we can derive the optimal time and power allocation parameters for the secrecy energy efficiency maximization problem for $K$ ($K \geq 3$) STs.

V. Simulation Results

In this section, we will simulate and illustrate the proposed scheme. In the simulation, the Rayleigh fading channel model is utilized to model the wireless channels. In addition, the path loss parameter is set to 3, and $T = 1$. For the target transmission rate and the target secrecy rate, we set $R_b = 1$ bit/s/Hz and $R_s = 0.5$ bit/s/Hz. Regarding to the nonlinear energy harvesting model, we set the parameters according to [28]. Moreover, we also simulate the linear harvesting model for comparison. In the following, we will give the results about the secrecy energy efficiency and the secrecy rate.

In Fig. 3, we simulate the secrecy energy efficiency of the proposed scheme versus the transmit power $p_i$. As shown in Fig. 3, the secrecy energy efficiency is not a monotonic function of the transmit power $p_i$. The reason is that when $p_i$ is low, there is limited power for energy harvesting which limits the increase of the secrecy energy efficiency; when $p_i$ is high, the secrecy rate is constrained by the target transmission rate. In addition, we can observe that the secrecy energy efficiency of the linear energy harvesting model is slight higher than the nonlinear energy harvesting model. However, when $p_i$ is large, the secrecy energy efficiency of the linear energy harvesting model is lower than the nonlinear energy harvesting model. The reason is that in the linear energy harvesting model, the secondary user can harvest more power for the secrecy transmission and the secrecy rate is constrained by the target transmission rate. In Fig. 3, we can also observe that more secondary users will introduce much more interference which leads to the decrease of the secrecy energy efficiency.

In Fig. 4, we show the secrecy energy efficiency of the proposed scheme versus the target transmission rate $R_b$. From Fig. 4, we can observe that the secrecy energy efficiency is a monotonic decreasing function with respect to $R_b$. The reason is that a large value of $R_b$ indicates that it is difficult to successfully transmit the privacy information and the secrecy energy efficiency will decrease. Similarly, we can also observe the secrecy energy efficiency of the linear energy harvesting model is higher than the nonlinear energy harvesting model, and more secondary users will lead to the decrease of the secrecy energy efficiency.

Fig. 5 shows the secrecy rate of the proposed scheme versus the transmit power $p_i$. From Fig. 5, we can see that the secrecy rate is a monotonic increasing function of $p_i$. 

\[
\text{EE}_i = \frac{R_s (1-p_{1,s,o})}{p_1 + p_c}, \ldots, \frac{R_s (1-p_{K,s,o})}{p_K + p_c}
\]

\[\text{s.t.} \ \tau_1 + \tau_2 = 1.
\]
The reason is that the increase of $p_t$ indicates that there will be more power for the secondary secure transmission and the secrecy rate will increase. When $p_t$ is very large, the target secrecy rate will limit the increase of the secrecy rate. And we can observe the secrecy rate of the nonlinear energy harvesting model is slightly lower than the linear energy harvesting model. In addition, we can also observe that the NOMA technique can improve the secrecy rate.

Fig. 6 shows the secrecy rate of the proposed scheme versus the target transmission rate $R_b$. In this figure, we can observe that the secrecy rate is a monotonic decreasing function of $R_b$. The reason is that the increase of $R_b$ indicates that it is hard to successfully transmit the privacy information and the secrecy rate will decrease. From Fig. 6, we can observe the secrecy rate of the nonlinear energy harvesting model is slightly lower than the linear energy harvesting model. In addition, we can also observe that the NOMA technique can improve the secrecy rate.

VI. Conclusion

In this paper, we propose a NOMA based secure transmission scheme in cognitive radio networks with nonlinear energy harvesting. In the proposed scheme, the secondary users are powered by the radio-frequency signal with nonlinear energy harvesting model, and then employ the NOMA technique to securely transmit the uplink privacy information. For the two secondary users and more than two secondary users scenarios, we provide comprehensive analysis of the secrecy performances, and derive the closed-form expressions of the secrecy outage probability. In the following, we develop the optimization problem to allocate the time slot and uplink transmit power such that the minimum secrecy energy efficiency rate is maximized. A two stages algorithm is proposed to solve the above optimization problems. Numerical results are presented to verify the analysis in terms of the secrecy rate and secrecy energy efficiency.

References


