Secrecy Performance Analysis of SWIPT System Based on OFDM Assisted Interference

Mei Qin(✉), Weidang Lu, Hong Peng, and Zhijiang Xu

College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China
1819510836@qq.com

Abstract. In this paper, we consider the security communications in an OFDM - based SWIPT system by adding a full-duplex, friendly jammer with wireless powered equipment between a transmitter (Tx) and an information receiver (IR) and an energy receiver (ER) which called (regarded as) a potential eavesdropper. We propose a scheme that under friendly jammer protection TX sends source messages to IR and jammer, the jammer sends jammer signal to ER and IR while receiving information from Tx to confound potential eavesdroppers but can be eliminated at IR. Our goal is to maximize the sum secrecy information rate by jointly optimizing the power allocation at the Tx and jammers while satisfying the energy harvesting at the ER.

Keywords: OFDM · SWIPT · Cooperative jamming (CJ)
Resource allocation

1 Introduction

Wireless Information and Power Transmission (WIPT) is an energy harvesting technology that addresses energy supply issues in network communications by eliminating the need for frequent battery charging and replacement. But the channel is open, it may be subjected to information theft. This paper proposes that there are several notable features of confidential wireless messaging and SWIPT over traditional secure communications. First, there is a potential for eavesdropping of wireless power transmission because the potential eavesdropper's power receiver is usually shorter than the information receiver Visit distance. Second, a lot of data prove that SWIPT also can enhance the security and reliability of wireless communications [1–3].

A SWIPT system basically includes an access point (AP) with a constant power supply and broadcasted broadcast signals to a group of user terminals, some of which are mainly used to decode information called the information receiver (IR), While others collect energy from the surrounding radio signals, known as the energy receiver (ER). However, since the ER is closer to the AP, it may eavesdrop on the valid information sent to the IR. And this will pose a huge challenge to the wireless secure communication [4].

In recent years, the confidentiality of the physical layer has become a new method for improving the information security of wireless networks, attracting many scientists

L. Meng and Y. Zhang (Eds.): MLICOM 2018, LNICST 251, pp. 391–399, 2018.
https://doi.org/10.1007/978-3-030-00557-3_39

began to study in this area. The physical layer of secure communication has two main types of interference: Cooperative jamming and adding artificial noise.

In [5, 6], the authors propose to confuse and reduce the eavesdropper's channel by adding artificial noise to ensure the confidential transmission of transmitter information. In the presence of one or more eavesdroppers, multiple relay collaborations are used to solve a secure communication from a source node to a destination node in [7]. and based on the RF-EH system, the authors propose that choose the best transmission station and ensure safe transmission in the presence of a source node and multiple eavesdroppers [8]. In [4, 9, 10], some researchers proposed adding artificial noise or Jammer so that ensure the security communication of the IR and maximize the secrecy rate of the IR while meeting the minimum energy receiving requirements of the ER.

The technique of creating interference on the eavesdropper's reception to reduce the associated links appears to be an effective method in practical applications in [11–13]. In [14], the author proposes a relay option to interrupt the security cooperation network to increase security against eavesdroppers. The first relay assists the source in transmitting the data to the destination by decoding the forwarding strategy. The second relay is used to send interference to the eavesdropper node to protect the destination node from interference and eavesdropping and prevent eavesdroppers from intercepting information.

In this article, we consider a secure communications transmission in an OFDM-based SWIPT system, which consists of an IR, a jammer, a Tx and an ER (potential eavesdropper), as shown in Fig. 1. We assume that Tx is a device with a constant energy supply and jammer does not have a constant energy supply and can only harvest energy from Tx. All devices are single antennas except that the jammer is a dual antenna and the jammer side receiving information from Tx while sending its own interference information to the ER and the IR, assuming equal power allocation above each subcarrier, the transmit power above each subcarrier at Tx and jammer is equal power allocated, with minimal energy acceptance, we optimize the system's security rate by jointly optimizing the power distribution factor of ER at Tx and jammer.

Although there are some similarities between our network settings and those used in [15] in terms of wirelessly powered dual-antenna jammers to confuse eavesdroppers. The research questions in our study are essentially different, especially when considering that the energy receiver ER is accepting data from the signals sent by Tx and Jammer are processed differently. The main innovations of our article can be summarized in several ways:

(1) Environmental Design: This article considers the case of eavesdropping using wireless CJ jamming machine to protect the communication between the source node and the destination node, we consider cooperative jamming (CJ) schemes, CJ adopts the full-duplex mode, it sends interference information to ER and IR while harvest energy from source information. The total power that CJ can transmit depends on the energy that it receives. Eavesdroppers eavesdrop on the information sent by the source node will also harvest the jammer to send the interference signal, we use the power distribution protocol, part of the eavesdropper used to intercept the information, part of the energy used to receive the source node and the jammer signal eavesdroppers have this configuration, however, the interference information received at the destination node can be ignored

by some mechanism [6]. With our network setup, you can maximize the transmission of your system's confidential information.

(2) Performance Evaluation: In order to see the proposed protocol confidentiality performance, we can see the impact on the system performance by changing the different parameters of the system, such as the distance between the jammer and the source node and the sending power of the source node.

2 System Model

We assume an OFDM-based secrecy communication scenario for SWIPT, as shown in Fig. 1, there are four-node system, consisting of one Tx, one jammer, one ER (potential eavesdropper) and one IR. The Tx, IR, and ER are set to single antenna while the jammer is dual antenna with one of them is used to receive energy and the other is used to transmit interference signal. When the Tx sends original information to the IR, the ER can harvest energy and eavesdrop information from the information source. At the same time, the jammer transmits interfering signals to IR and ER while receiving energy from original information, since it is a full-duplex mode of operation, we assume that the interference between the two antennas is negligible. It is noteworthy that the interference signal from the jammer is not only used to interfere with ER but also to ER as an energy source. We assume that the system has N subcarriers. The channel power gain of $Tx \rightarrow IR$, $Tx \rightarrow ER$, $Tx \rightarrow jammer$ are expressed as $h_{I,n}$, $h_{E,n}$, and $h_{J,n}$, also the channel power gain from jammer to IR and ER are expressed as $g_{I,n}$, $g_{J,n}$.

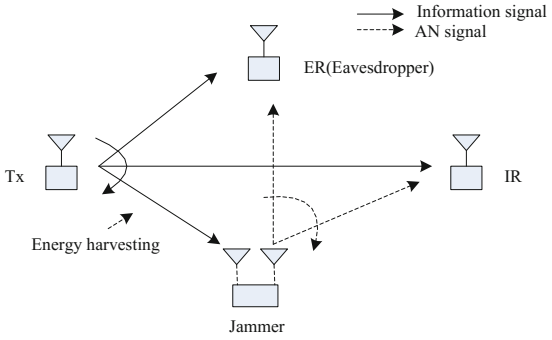

Fig. 1. System model of the wireless-powered secrecy SWIPT

In this paper we assume that the total transmit power of the transmitter is P, and the transmit power of Tx on the SC n is p_n and the jammer on the SC n is q_n. We consider the constraint of peak power on p_n and q_n, $0 < p_n \leq \bar{p}_n, 0 < q_n \leq \bar{q}_n$, for $n = 1, \ldots, N$. The total transmit power at the Tx is thus given by

$$\sum_{n=1}^{N} p_n \leq P \tag{1}$$

Since the jammer harvests energy at the original information sent by the Tx, the transmit power constraint at the jammer can be expressed as:

$$\sum_{n=1}^{N} q_n \leq \zeta \sum_{n=1}^{N} p_n h_{J,n} \tag{2}$$

where ζ is a constant that account for the energy conversion efficiency, in order to simplify the calculation of the next we assume that $\zeta = 1$.

Energy received by the energy receiver ER comes from two parts, one from Tx, and the other from jammer, the harvested power should reach the minimum energy requirement $\bar{Q}_n$:

$$\sum_{n=1}^{N} \left((1-\alpha) p_n h_{E,n} + (1-\beta) q_n g_{E,n}\right) \geq \sum_{n=1}^{N} \bar{Q}_n \tag{3}$$

where $\bar{Q}_n$ is the minimum energy requirement that the ER should satisfy on SCn.

In this paper, we assume that the interfering signal sent by jammer can be removed at IR but can not at ER, so the rates of information obtained at classes IR and ER, respectively, can be expressed as:

$$r_n = \log\left(1 + \frac{p_n h_{I,n}}{\sigma^2}\right), r_n^e = \log\left(1 + \frac{\alpha p_n h_{E,n}}{\sigma^2 + \beta q_n g_{E,n}}\right) \tag{4}$$

The achievable information secrecy rate for R_n on SCn can be expressed as:

$$R_n = \left[r_n - r_n^e\right]^+ = \left[\log\left(1 + \frac{p_n h_{I,n}}{\sigma^2}\right) - \log\left(1 + \frac{\alpha p_n h_{E,n}}{\sigma^2 + \beta q_n g_{E,n}}\right)\right]^+ \tag{5}$$

for all $n \in N$, where $[\bullet]^+ \triangleq \max(0, \bullet)$.

In such jammer and eavesdropper model, we aim to jointly optimize the power p_n and q_n, and power distribution ratio α, β, while ensuring that the constraints (1)–(3) condition is established. Our optimization problem can be expressed as:

$$(P1): \max_{\{\alpha,\beta,p_n,q_n\}} \sum_{n=1}^{N} R_n \tag{6}$$

$$s.t. \qquad (1) - (3) \tag{6a}$$

$$0 \leq \alpha \leq 1, 0 \leq \beta \leq 1 \tag{6b}$$

$$0 \leq p_n \leq \bar{p}, 0 \leq q_n \leq \bar{q} \tag{6c}$$

3 The Problem Formulation and Solution

First, we need to find the optimal α^*, β^*, in order to ensure $R_n > 0$ in (5) and satisfy the constraints of (3), the range of β can be expressed as:

$$\beta_1 \leq \beta \leq \beta_2 \tag{7}$$

where

$$\beta_1 = \frac{\sigma^2(\alpha h_{E,n} - h_{I,n})}{h_{I,n} q_n g_{E,n}}, \beta_2 = \frac{(1-\alpha) p_n h_{E,n} + q_n g_{E,n} - \bar{Q}_n}{q_n g_{E,n}}$$

union (6c) and (7) we can get the value of α range is given by:

$$\alpha \geq \alpha_2, \alpha \geq \alpha_1, \alpha \leq \alpha_3$$

where

$$\alpha_1 = \frac{h_{I,n}}{h_{E,n}}, \alpha_2 = 1 - \frac{\bar{Q}}{p_n h_{E,n}}, \alpha_3 = \frac{h_{I,n}(p_n h_{E,n} + q_n g_{E,n} - \bar{Q} + \sigma^2)}{h_{E,n}(\sigma^2 + p_n h_{I,n})}$$

On the other hand, we derive the partial derivative of α and β in (5), we can get

$$\begin{cases} \frac{\partial R_n}{\partial \alpha} = \frac{-p_n h_{E,n}}{(\sigma^2 + \beta q_n g_{E,n} + \alpha p_n h_{E,n}) \ln 2} < 0 \\ \frac{\partial R_n}{\partial \beta} = \frac{\alpha p_n h_{E,n} q_n g_{E,n}}{(\sigma^2 + \beta q_n g_{E,n} + \alpha p_n h_{E,n})(\sigma^2 + \beta q_n g_{E,n}) \ln 2} > 0 \end{cases}$$

Obviously, R_n is monotonically decreasing with α, and R_n is monotonically increasing with β, therefore, there are two cases for the value of α.

Case1. When $\alpha_1 > \alpha_2$, then we can obtain $\alpha_1 \leq \alpha \leq \alpha_3$, and the optimal α^*, β^* are given by

$$\alpha^* = \alpha_1, \beta^* = \beta_2 \tag{8}$$

Case2. When $\alpha_1 \leq \alpha_2$, we can get $\alpha_2 \leq \alpha \leq \alpha_3$, the optimal α^*, β^* are given by

$$\alpha^* = \alpha_2, \beta^* = 1 \tag{9}$$

4 Simulation Results

In this section, we use experimental data to verify the performance of our proposed CJ scheme system. we assuming equal power allocation at Tx and CJ on SCs, $p_{k,n} = P/N$, $q_{k,n} = p_{k,n}/h_{J,n}$, here we drop index n and k of $p_{k,n}$, $q_{k,n}$ for brevity, System parameters are set as $N = 32$, the noise power $\sigma^2 = -60$ dBm, and the pass-loss exponent is 2.

The jammer, IR and Tx are in the same straight line and the distance from Tx to IR is 6 m. The jammer moves between Tx and IR, and we denote the distance from Tx to jammer as $d1$, in addition, we assume that the distance from Tx to ER is 3 m with 30°.

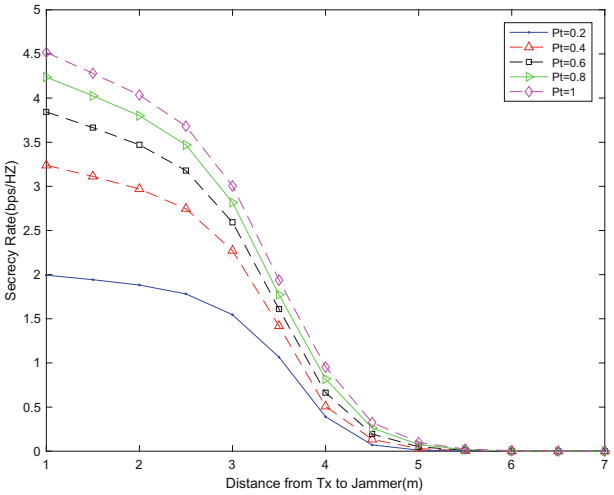

Fig. 2. Secrecy rate versus d1(m), with $\bar{Q} = -40$ dbm

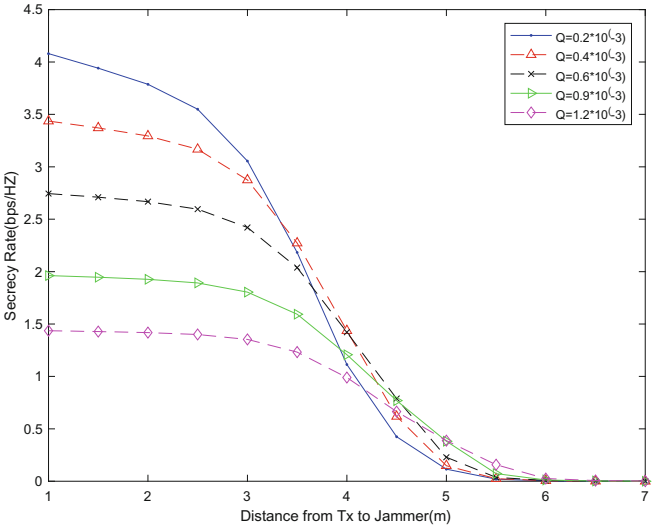

Fig. 3. Secrecy rate versus d1(m), with $P = 30$ dbm

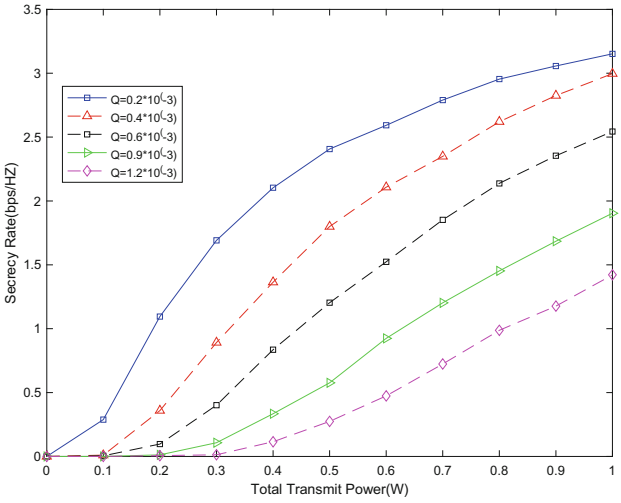

Fig. 4. Secrecy rate versus total power P(W), with $d1 = 3$ m

Figures 2 and 3 show the impact of minimum energy reception requirements $\bar{Q}$ and the total transmit power P of the source node on the system's secrecy rate. The $\bar{Q}$ set as $\bar{Q} = -40$ dbm in Fig. 2, and the total transmit power set as $P = 30$ dbm, it can be seen from Fig. 2 that the confidentiality of the system decreases with the increase of the distance from the source node of the jammer. However, it can be seen from Fig. 3 that the confidentiality of the system does not increase with the increase of the minimum energy receiving requirement, In the case of short distances (d1 < 2 m), the confidentiality of the system will increase as the energy receiving requirements decrease.

Figure 4 demonstrate the effect of the fraction of the total power P on the system's security rate, and it can be observed that the security rate of system can be improved by increasing P or reduce the distance from jammer to Tx. We can see that when the distance is increased to 5 m, the system's secrecy rate is very small, and this result is consistent with the result in Figs. 2 and 3.

Figure 5 depict the optimal power distribution factor versus source node transmit power, and we can see the effect of transmit power and the harvested energy constraint on α^*, β^* with $d1 = 3$ m, from Fig. 4, we can see that when the transmission power is constant, the system's information security rate will decrease with the increase of the receiving energy constraint. Therefore, in combination with Fig. 3, we can obtain: by reducing the receiving energy constraint, increasing the transmission power and reducing the distance from Tx to jammer to improve the system's information security rate.

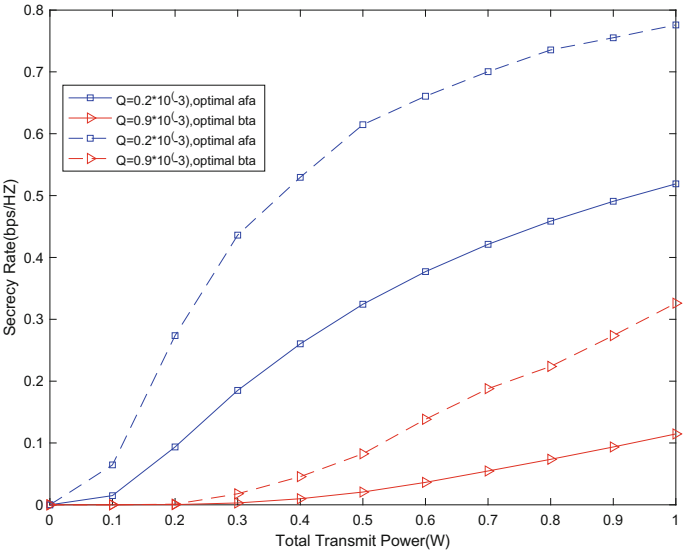

Fig. 5. Optimal versus total power P(W), with $d1 = 3$ m

5 Conclusion

We propose a scheme for OFDM-based SWIPT systems to maximize the security of system secrets with a friendly jammer. In addition, we describe the effect of certain parameters on the security rate of the system. According to our theoretical analysis, we can get the result that when the total transmit power increases or the short-distance distance decreases, the system security and confidentiality Better. Numerical analysis of the theory also shows that compared with the method without CJ, our scheme obviously improves the performance of the system. Our results also prove that optimized performance is better.

References

1. Chen, X., Ng, D.W.K., Chen, H.H.: Secrecy wireless information and power transfer: challenges and opportunities[M]. IEEE Press (2016)
2. Varshney, L.R.: Transporting information and energy simultaneously. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 1612–1616, Toronto, ON, CA, July 2008
3. Grover, P., Sahai, A.: Shannon meets Tesla: wireless information and power transfer. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Austin, TX, USA, pp. 2363–2367, June 2010
4. Xing, H., Wong, K.K., Chu, Z., et al.: To harvest and jam: a paradigm of self-sustaining friendly jammers for secure AF relaying. IEEE Trans. Signal Process. **63**(24), 6616–6631 (2015)

5. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. IEEE Trans. Wirel. Commun. **7**(6), 2180–2189 (2008)
6. Zhang, M., Liu, Y., Zhang, R.: Artificial noise aided secrecy information and power transfer in OFDMA systems. IEEE Trans. Wirel. Commun. **15**(4), 3085–3096 (2016)
7. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
8. Vo, V.N., Nguyen, T.G., So-In, C., et al.: Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer. IEEE Access **PP**(99), 1 (2017)
9. Bi, Y., Chen, H.: Accumulate and jam: towards secure communication via a wireless-powered full-duplex jammer[J]. IEEE J. Sel. Top. Signal Process. **10**(8), 1538–1550 (2016)
10. Liu, W., Zhou, X., Durrani, S., et al.: Secure communication with a wireless-powered friendly jammer. IEEE Trans. Wirel. Commun. **15**(1), 401–415 (2016)
11. Simeone, O., Popovski, P.: Secure communications via cooperating base stations. IEEE Commun. Lett. **12**, 188–190 (2008)
12. Popovski, P., Simeone, O.: Wireless secrecy in cellular systems with infrastructure-aided cooperation. Trans. Inf. Forensics Secur. **4**, 242–256 (2009)
13. Tekin, E., Yener, A.: The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming. IEEE Trans. Inf. Theory **54**, 2735–2751 (2008)
14. Krikidis, I., Thompson, J.S., Mclaughlin, S.: Relay selection for secure cooperative networks with jamming. IEEE Trans. Wirel. Commun. **8**(10), 5003–5011 (2009)
15. Liu, M., Liu, Y.: Power allocation for secure SWIPT systems with wireless-powered cooperative jamming. IEEE Commun. Lett. **PP**(99), 1 (2017)