When Friendly Jamming Meets Wireless Energy Transfer

Qi Sun*, Hong-Ning Dai*, Qiu Wang*, Xuran Li* and Hao Wang†
Macau University of Science and Technology, Macau SAR
xatusun@189.cn; hndai@ieee.org; qiu_wang@foxmail.com; lxrget@163.com
†Norwegian University of Science and Technology, Aalesund, Norway
hawa@ntnu.no

***Abstract*—Friendly-jamming schemes can effectively reduce the eavesdropping risk in wireless networks by generating sufficient interference to prevent eavesdroppers from snooping confidential communications. However, this type of anti-eavesdropping schemes can also affect the normal communications due to the interference to legitimate users. On the other hand, Wireless Energy Transfer (WET) technology has received much attention recently since WET allows a node to obtain the energy from electromagnetic radiation. In this paper, we integrate the friendly-jamming scheme with WET. We call this scheme as Wireless-Jamming-Energy-Transfer (WJET). This scheme can translate the harmful interference radiated from jammers into the energy harvested by legitimate transmitters. In order to evaluate the effectiveness of this scheme, we establish an analytical model to analyze the transmission probability and the eavesdropping probability. Simulations verify that WJET scheme can simultaneously decrease the eavesdropping probability of eavesdroppers and increase the transmission probability of legitimate users. In addition, we investigate the density of jammers to achieve the optimal transmission probability according to various channel conditions, the density of transmitters and the transmission power of jammers.**

I. Introduction

Due to the broadcast feature of wireless communications, wireless communications are more vulnerable to malicious attacks. How to improve the security of wireless network becomes a crucial issue with the proliferation of wireless networks and wireless services [1]. Since most of malicious attacks often require wiretapping (aka eavesdropping) confidential communications, extensive attention has been paid to designing anti-eavesdropping schemes [2]. Recently, anti-eavesdropping schemes by generating interference radiated from jammers to eavesdroppers have received extensive attention. This type of anti-eavesdropping schemes are named as friendly jamming schemes. The main idea of friendly-jamming schemes is to increase the noise level at the eavesdropper so that the eavesdroppers cannot successfully wiretap the confidential information [3]–[5]. The benefits of friendly-jamming schemes include that there is no requirement for computing capability of nodes and no necessity of centralizing security schemes [6]. Friendly-jamming schemes have been used in various network scenes to decease the possibility of eavesdropping [7]–[9]. However, interference signals emitted by friendly jammers can reversely affect the normal communication of legitimate users. In this regard, many research efforts have been proposed to reduce the impact on legitimate communications by introducing different types of jammers, including constant jammers, intermittent jammers, adaptive jammers, reactive jammers and intelligent jammer [4], [10], [11]. Moreover, another solution is to calculate and optimize the location of the jammers to find the way to minimize the impact on legitimate communications [12]. But most of them require channel state information (CSI) of eavesdroppers while it is difficult to obtain CSI since eavesdroppers are usually passive and they do not generate any CSI.

On the other hand, Wireless Energy Transfer (WET) allows that nodes in a network can be charged by receiving wireless signal [13]. Compared with conventional battery-powered communication networks, the introduction of WET improves the performance in many aspects, such as higher throughput [14], longer device lifetime and lower network operating cost [15]. Because of these advantages of WET, many previous studies consider using it in various types of networks, e.g., WET is used to charge mobile terminals in cellular networks [16] and to harvest wireless devices in Internet of Things (IoT) [13].

The WET technology allows us to investigate friendly jamming schemes in a different aspect. Unlike most of previous studies in friendly-jamming schemes in which jamming signal is regarded as harmful to legitimate communications [17], [18], jamming signal can be regarded as an energy source to potentially harvest energy for legitimate users. Therefore, we propose a joint scheme by integrating the friendly-jamming scheme with WET. We call this scheme as Wireless-Jamming-Energy-Transfer scheme (WJET). In WJET, friendly jamming can mitigate the eavesdropping probability of eavesdropper by sending interference. On the other hand, the radio signal radiated from friendly jammers can harvest the legitimate users.

To the best of our knowledge, this is the first study in investigating the integration of friendly-jamming scheme with WET in wireless networks. The contribution of this paper can be summarized as follows.

- We formally propose a WJET scheme. In particular, we establish an analytical model to evaluate the performance of WJET in terms of the transmission probability and the

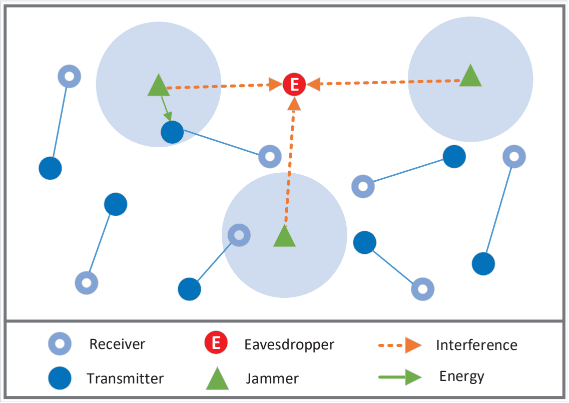


Fig. 1. Network model

eavesdropping probability.

- We conduct extensive simulations to verify the accuracy of our proposed models. We observe that WJET not only deceases the eavesdropping probability, but also increases the transmission probability of legitimate users.
- We derive the optimal density of jammers in order to achieve the optimal transmission probability. The results show that we can obtain the optimal transmission probability by adjusting the density of jammers based on various channel conditions, the density of transmitters and the transmission power of jammers.

The remaining paper is organized as follows. We first present the system model in Section II. Section III then presents the analysis of transmission and eavesdropping activity. We next show the simulation results in Section IV. Section V presents the optimal solution of transmission probability. Finally, the paper is concluded in Section VI.

II. System Models

A. Network Model

Fig. 1 presents the network model of this paper. We assume that the network plane is infinite and the border effect is ignored. In this network, both legitimate transmitters and receivers are arranged according to homogeneous Poisson point process (HPPP) with intensity λ_t. There is an eavesdropper in this network trying to eavesdrop the transmission between legitimate users. To interfere with the eavesdropping process to protect the confidential transmission from legitimate users, friendly-jammers are introduced. These friendly-jammers are distributed according to HPPP of intensity λ_j. We assume that friendly-jammers can continuously radiate radio signals, which can be used to interfere with eavesdroppers and also be used to charge transmitters.

B. Channel Model

In our channel model, radio signals are assumed to experience both Rayleigh fading and path loss. Let the power of transmitters is denoted by P_t. Then, the received power at a receiver is $P_t h r^{-\alpha}$, where α is the path loss factor, h is a Rayleigh fading factor following an exponential distribution with mean 1 ($h \sim \exp(1)$), and r is the distance between a receiver and a transmitter.

Based on the channel model, we then consider the Signal to Interference plus Noise Ratio (SINR) model. The SINR at the receiver is expressed as

$$\text{SINR} = \frac{P_t h r^{-\alpha}}{\sigma^2 + I_j + I_t}, \tag{1}$$

where σ^2 is the noise power, $I_j = \sum\limits_{m \in \Phi_1} P_j h_m R_m^{-\alpha}$ denotes the cumulative interference from all the jammers, Φ_1 denotes the set of jammers, R_m is the distance from the mth jammer to the tagged receiver, and h_m is the Rayleigh fading factor between the mth jammer and the tagged receiver ($h_m \sim \exp(1)$). The term of $I_t = \sum\limits_{i \in \Phi_2 / t_0} P_t h_i R_i^{-\alpha}$ denotes the cumulative interference from all the transmitters (except for the tagged transmitter denoted by t_0), and Φ_2 denotes the set of transmitters, R_i is the distance between the ith transmitter and the tagged receiver, and h_i is the Rayleigh fading factor between the ith transmitter and the tagged receiver ($h_i \sim \exp(1)$).

III. Analysis of Transmission and Eavesdropping Activity

A. Problem definition

In this paper, we use jammers in networks to fulfill two purposes: 1) charging transmitters with energy and 2) decreasing the eavesdropping possibility. Therefore, we consider both the transmission probability and the eavesdropping probability to evaluate the performance of our proposed scheme. Specifically, the transmission probability and the eavesdropping probability are defined as follows, respectively,

Definition 1: Transmission probability is the probability that a transmitter can successfully communicate with its receiver.

Definition 2: Eavesdropping probability is the probability that a eavesdropper can tap information from the nearest transmitter.

Then, we analyze the transmission probability in Section III-B and the eavesdropping probability in Section III-C.

B. Analysis on Transmission Probability

In our network, a transmitter can successfully transmit if and only if it satisfies both the following conditions:

1) The transmitter has the energy for its transmission;
2) The transmitter can connect with the its receiver successfully.

Based on the above conditions, the transmission probability, denoted by $\mathbb{P}_t$, can be expressed as follows,

$$\mathbb{P}_t = \mathbb{P}_h \mathbb{P}_s, \tag{2}$$

where $\mathbb{P}_h$ is the average probability that a transmitter has the energy to transmit, $\mathbb{P}_s$ is the probability that a transmitter can successfully connect with its receiver. Note that the initial state of power of transmitters is assumed to be empty. Hence, in order to transmit, the transmitter needs to be charged by radio signals radiated from jammers. We assume that the transmitter can be only charged from the nearest jammer. This is because the power received by transmitters should be large enough to activate the energy harvesting circuit.

We first consider the average probability that a transmitter has the energy P_h. We assume that a transmitter can only be charged by the nearest jammer if the received power at the transmitter is greater than a given threshold θ. Then $\mathbb{P}_h$ can be expressed as

$$\begin{aligned}\mathbb{P}_h =&E_{r_j}\left[\mathbb{P}\left(P_j h_0 {r_j}^{-\alpha} > \theta \middle| r_j\right)\right]\\ =&\int_0^{\infty} \mathbb{P}\left(P_j h_0 {r_j}^{-\alpha} > \theta \middle| r_j\right) f(r_j) dr_j,\end{aligned} \tag{3}$$

where r_j is the distance between the transmitter and the nearest jammer, and $f(r_j)$ is the probability density function (PDF) of r_j. Since jammers follow HPPP, the cumulative distribution function (CDF) of r_j is $\mathbb{P}[r_j \leq R] = 1 - e^{-\lambda\pi R^2}$. Hence, we can have $f(r_j)$ as follows,

$$f(r_j) = 2\pi\lambda_j r_j e^{-\lambda_j r_j^2 \pi}. \tag{4}$$

After combining with Eq. (4), we can express Eq. (3) as

$$\begin{aligned}\mathbb{P}_h =& \int_0^{\infty} \left(e^{-P_j^{-1} {r_j}^{\alpha}\theta}\right)\left(e^{-\lambda_j r_j^2 \pi} 2\pi\lambda_j r_j\right) dr_j\\ =& \int_0^{\infty} 2\pi\lambda_j r_j e^{-(P_j^{-1} {r_j}^{\alpha}\theta + \lambda_j r_j^2 \pi)} dr_j.\end{aligned} \tag{5}$$

Next, we analyze the transmission probability $\mathbb{P}_s$ that a transmitter can successfully communicate with a receiver. We require $SINR > \beta$ at a receiver to ensure the legitimate transmission.

We denote the distance between a transmitter and its receiver by r. We assume that each transmitter communicates with the the nearest receiver. Since receivers follow HPPP, the PDF of r can be calculated with similar approach with the PDF of r_j in Eq. (4) as $f(r) = 2\pi\lambda_t r e^{-\lambda_t r^2 \pi}$. Then the probability that a transmitter can successfully communicate with its receiver $\mathbb{P}_s$ is given as follows,

$$\begin{aligned}\mathbb{P}_s =& E_r[\mathbb{P}(\mathrm{SINR} > \beta | r)]\\ =& \int\limits_{r>0} \mathbb{P}\left[\frac{P_t h r^{-\alpha}}{\sigma^2 + I_t + I_j} > \beta | r\right] e^{-\lambda_t \pi r^2} 2\pi\lambda_t r dr\\ =& \int\limits_{r>0} \mathbb{P}[h > \beta r^{\alpha}(\sigma^2 + I_t + I_j){P_t}^{-1} | r] e^{-\lambda_t \pi r^2} 2\pi\lambda_t r dr.\end{aligned} \tag{6}$$

Since h is a random variable following an exponential distribution with mean 1, Eq. (6) can be expressed as

$$\begin{aligned}\mathbb{P}[\mathrm{SINR} > \beta] =& E_{I_t, I_j}\left[\mathbb{P}[h > \beta r^{\alpha}(\sigma^2 + I_t + I_j){P_t}^{-1}]\right]\\ =& E_{I_t, I_j}\left[\exp(-\beta r^{\alpha}(\sigma^2 + I_t + I_j){P_t}^{-1})\right]\\ =& e^{-{P_t}^{-1}\beta r^{\alpha}\sigma^2} \cdot E_{I_t, I_j}[e^{-\beta r^{\alpha}(I_t + I_j){P_t}^{-1}}]\\ =& e^{-{P_t}^{-1}\beta r^{\alpha}\sigma^2} \cdot L_{I_j}({P_t}^{-1}\beta r^{\alpha}) \cdot L_{I_t}({P_t}^{-1}\beta r^{\alpha}),\end{aligned} \tag{7}$$

where $L_A(a)$ denotes the Laplace transform of random variable of A at a.

Let $s = {P_t}^{-1}\beta r^{\alpha}$, then the Laplace transform $L_{I_j}({P_t}^{-1}\beta r^{\alpha})$ in Eq. (7) can be calculated as

$$\begin{aligned}L_{I_j}(s) =& E_{I_j}[e^{-sI_j}]\\ =& E_{\Phi_1, \{h_m\}}\Big[\exp(-s \sum_{m\in\Phi_1} P_j h_m R_m^{-\alpha})\Big]\\ =& E_{\Phi_1}\Big[\prod_{m\in\Phi_1} E_{h_m}[\exp(-sP_j h_m R_m^{-\alpha})]\Big]\\ =& E_{\Phi_1}\left[\prod_{m\in\Phi_1} \frac{1}{1 + sP_j R_m^{-\alpha}}\right],\end{aligned} \tag{8}$$

where the last but one step is obtained from the fact that random variables h_m and R_m are mutually independent and Rayleigh fading variable h_m is i.i.d. for $m \in \Phi_1$, and the last step is obtained from the fact that $h_m \sim \exp(1)$.

According to the property of the probability generation function of a PPP (denoted by Φ) in a space S: for a function $0 < f(x) < 1$ $(x \in \Phi)$, $\mathbb{E}[\prod_{x\in\Phi} f(x)] = \exp\left(-\lambda \int_S (1 - f(x))dx\right)$ [19], we can express Eq. (8) as follows,

$$L_{I_j}(s) = \exp\left(-2\pi\lambda_j \int_0^{\infty} (1 - \frac{1}{1 + sP_j v^{-\alpha}})vdv\right). \tag{9}$$

Then, we have

$$\begin{aligned}L_{I_j}({P_t}^{-1}\beta r^{\alpha}) =& \exp\left(-2\pi\lambda_j \int_0^{\infty} (\frac{\beta}{\beta + P_t {P_j}^{-1}(v/r)^{\alpha}})vdv\right)\\ =& \exp\left(-\pi(P_t^{-1} P_j)^{2/\alpha} r^2 \lambda_j \rho_1\right),\end{aligned} \tag{10}$$

where $\rho_1 = \beta^{2/\alpha}\int_0^{\infty} \frac{1}{1 + u_1^{\alpha/2}} du_1$, and $u_1 = \left(\frac{v}{r(\beta P_t^{-1} P_j)^{1/\alpha}}\right)^2$.

Since the transmitters are subject to the same distribution as jammers (i.e., HPPP), using the similar approach to the calculation of $L_{I_j}({P_t}^{-1}\beta r^{\alpha})$, we can calculate the other Laplace transform $L_{I_t}({P_t}^{-1}\beta r^{\alpha})$ in Eq. (7) as follows,

$$\begin{aligned}L_{I_t}(s) =& E_{I_t}[e^{-sI_t}]\\ =& E_{\Phi_2, \{h_i\}}\Big[\exp(-s \sum_{i\in\Phi_2/b_0} P_t h_i R_i^{-\alpha})\Big]\\ =& E_{\Phi_2}\left[\prod_{i\in\Phi_2/b_0} \frac{1}{1 + sP_t R_i^{-\alpha}}\right]\\ =& \exp\left(-2\pi\lambda_t \int_0^{\infty} (1 - \frac{1}{1 + sP_t v^{-\alpha}})vdv\right).\end{aligned} \tag{11}$$

Then, we have

$$L_{I_t}({P_t}^{-1}\beta r^{\alpha}) = \exp\left(-\pi r^2 \lambda_t \rho_2\right), \tag{12}$$

where $\rho_2 = \beta^{2/\alpha}\int_0^{\infty} \frac{1}{1 + u_2^{\alpha/2}} du_2$ and $u_2 = \left(\frac{v}{r\beta^{1/\alpha}}\right)^2$.

By combining Eq. (12), Eq. (10) and Eq. (7), we can have the probability that a transmitter can successfully communicate with its receiver $\mathbb{P}_s$ as follows,

$$\mathbb{P}_s = \int_0^{\infty} 2e^{-P_t^{-1} r^{\alpha}\sigma^2\beta - \pi(P_t^{-1}P_j)^{2/\alpha} r^2 \lambda_t \rho_1 - \pi r^2 \lambda_j \rho_2} \pi r \lambda_t dr. \tag{13}$$

Finally, by combining Eq. (2), Eq. (3) and Eq. (13), we have the transmission probability $\mathbb{P}_t$ as follows,

$$\mathbb{P}_t = \int_0^\infty 2e^{-P_t^{-1} r^\alpha \sigma^2 \beta - \pi (P_t^{-1} P_j)^{2/\alpha} r^2 \lambda_t \rho_1 - \pi r^2 \lambda_j \rho_2} \pi r \lambda_t dr \cdot \int_0^\infty 2\pi \lambda_j r_j e^{-(P_j^{-1} {r_j}^\alpha \theta + \lambda_j r_j^2 \pi)} dr_j. \tag{14}$$

C. Analysis on Eavesdropping Probability

We assume that the eavesdropper can wiretap the information from the nearest transmitter if the SINR at the eavesdropper is greater than a given threshold T. Then, the eavesdropping probability $\mathbb{P}_e$ can be expressed as

$$\begin{aligned} \mathbb{P}_e =& E_{r_e} \left[\mathbb{P}[\text{SINR} > T | r_e] \right] \\ =& \int\limits_{r_e > 0} \mathbb{P} \left[\mathbb{P}[\text{SINR} > T | r_e] \, f(r_e) dr_e, \right. \end{aligned} \tag{15}$$

where r_e is the distance between the eavesdropper and the nearest transmitter, and $f(r_e)$ is the PDF of r_e. Since the transmitters follow HPPP, the PDF of r_e is $f(r_e) = e^{-\lambda_t \pi r_e^2} 2\pi \lambda_t r_e$.

Similar to the calculation procedure of the probability that a transmitter can successfully communicate with its receiver $\mathbb{P}_s$, $\mathbb{P}[\text{SINR} > T]$ can be expressed as

$$\begin{aligned} \mathbb{P}[\text{SINR} > T | r] =& \mathbb{P}\left[h > T r_e^\alpha (\sigma^2 + I_t + I_j) {P_t}^{-1} | r \right] \\ =& E_{I_t, I_j} \left[\mathbb{P}[h > T r_e^\alpha (\sigma^2 + I_t + I_j) {P_t}^{-1} | r] \right] \\ =& E_{I_t, I_j} \left[\exp[-T r_e^\alpha (\sigma^2 + I_t + I_j) {P_t}^{-1}] | r \right] \\ =& e^{-{P_t}^{-1} T r_e^\alpha \sigma^2} \cdot E_{I_t, I_j} [e^{-T r_e^\alpha (I_t + I_j) {P_t}^{-1}}] \\ =& e^{-{P_t}^{-1} T r_e^\alpha \sigma^2} \cdot L_{I_j}({P_t}^{-1} T r_e^\alpha) \cdot L_{I_t}({P_t}^{-1} T r_e^\alpha) \\ =& e^{-{P_t}^{-1} T r_e^\alpha \sigma^2 - \pi (P_t^{-1} P_j)^{2/\alpha} r_e^2 \lambda_t \rho_3 - \pi r_e^2 \lambda_j \rho_4}, \end{aligned} \tag{16}$$

where $\rho_3 = T^{2/\alpha} \int_0^\infty \frac{1}{1 + u_3^{\alpha/2}} du_3$, $u_3 = \left(\frac{v}{r_e (T P_t^{-1} P_j)^{1/\alpha}} \right)^2$, $\rho_4 = T^{2/\alpha} \int_0^\infty \frac{1}{1 + u_4^{\alpha/2}} du_4$ and $u_4 = \left(\frac{v}{r_e T^{1/\alpha}} \right)^2$.

After combining Eq. (16), and Eq. (10), Eq. (12) and Eq. (15), we can obtain the eavesdropping probability P_e as follows,

$$\mathbb{P}_e = \int\limits_{r_e > 0} 2\pi \lambda_t r_e e^{-{P_t}^{-1} T r_e^\alpha \sigma^2 - \pi (P_t^{-1} P_j)^{2/\alpha} r_e^2 \lambda_t \rho_3 - \pi r_e^2 \lambda_j \rho_4} dr_e. \tag{17}$$

IV. Simulation Results

In this section, we conduct simulations to verify the accuracy of our proposed model on the transmission probability and the eavesdropping probability. We use MATLAB as the simulation tool. In particular, transmitters, receivers and jammers are distributed according to HPPP in a plane of area 100×100. We consider the path loss factor α is ranging from 3 to 5 and the noise power $\sigma^2 = 0.1, P_t = 2, P_j = 1$. Each result of simulations is calculated by averaging over 10,000 simulation trials.

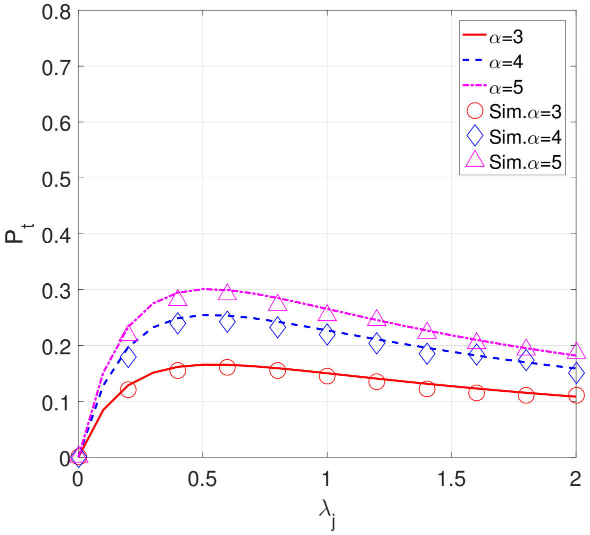


Fig. 2. Transmission probability $\mathbb{P}_t$ versus the intensity of jammers λ_j with different path loss α, where $\lambda_t = 0.5$, $\beta = 0.9, \theta = 0.9$.

A. Results on Transmission Probability

Fig. 2 shows the results of the transmission probability P_t with different path loss α. We can see that $\mathbb{P}_e$ increases when the path loss factor α increases from 3 to 5.

We can observe that P_t fluctuates with the intensity of jammers λ_j. Specifically, P_t increases first and then decreases with the increased λ_j. This can be explained as follows: when there are fewer jammers, transmitters have less chance to be harvested with the energy to transmit. With the increased number of jammers, transmitters can have higher probability to obtain the energy, resulting in the increase of $\mathbb{P}_t$. However, when the number of jammers increase further, the increased interference caused by jammers also hampers the legitimate communications. Therefore, this is a trade-off on choosing the number of jammers.

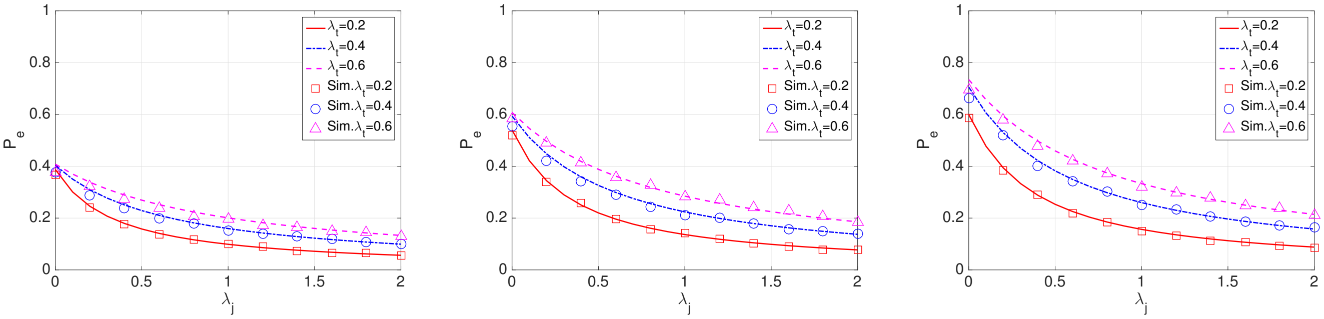
B. Results on Eavesdropping Probability

Fig. 3 shows the eavesdropping probability $\mathbb{P}_e$ with different values of path loss α. We can observe that when the path loss factor α increase from 3 to 5, $\mathbb{P}_e$ increases.

We next evaluate the impact of the intensity of jammers λ_j and the intensity of transmitters λ_t on the eavesdropping probability $\mathbb{P}_e$. When λ_t increases from 0.2 to 0.6, we can see that the $\mathbb{P}_e$ increases. Meanwhile, when λ_j increases from 0 to 2, $\mathbb{P}_e$ decreases significantly. In other words, the higher density of transmitters is, the more legitimate communications can be eavesdropped. One the other hand, the higher density of jammers is, the fewer legitimate communications can be eavesdropped (due to the higher interference to the eavesdropper).

V. The Optimal Solution of Transmission Probability

As shown in Fig. 2, the transmission probability increases first and then decreases with the increased intensity of jammers



(a) $\alpha = 3$ (b) $\alpha = 4$ (c) $\alpha = 5$

Fig. 3. Eavesdropping probability $\mathbb{P}_e$ versus the intensity of jammers λ_j with different intensity of transmitters λ_t, where $T = 1$.

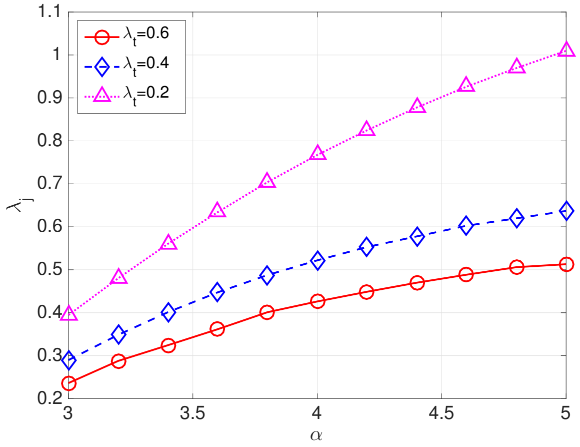


Fig. 4. Optimal intensity of jammers λ_j versus path loss factor α with different intensity of transmitters λ_t.

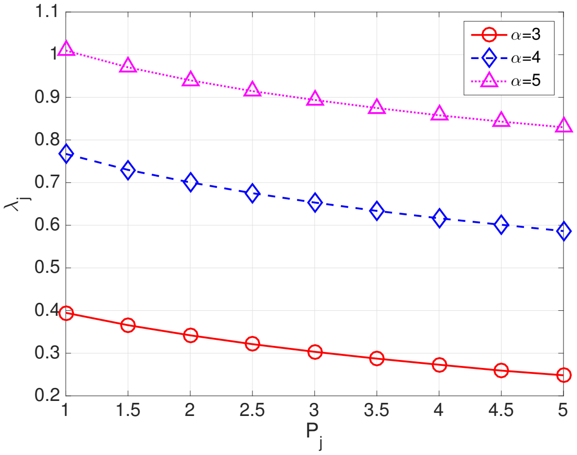


Fig. 5. Optimal intensity of jammers λ_j versus transmission power of jammers P_j with different path loss factor α.

λ_j, implying that we can have the optimal value of transmission probability by choosing an optimal intensity of jammers λ_j. Therefore, we investigate the relationship between the optimal intensity of jammers λ_j with different parameters. We first have the partial derivative of function $\mathbb{P}_t$ with respect to variable λ_j as shown in Eq. (18). Next we calculate the zero point of Eq. (18) by letting $\frac{\partial \mathbb{P}_t}{\partial \lambda_j} = 0$. Thus, we can have the optimal λ_j to achieve the optimal transmission probability.

Fig. 4 presents the results of optimal intensity of jammers λ_j versus path loss factor α with different intensity of transmitters λ_t. We can see that, to maintain the optimal transmission probability, the optimal λ_j increases when the path loss factor α increases from 3 to 5. This implies that when the transmission channel deteriorates, the number of jammers needs to be increased to guarantee the charging process to achieve the optimal transmission probability. In addition, when the intensity of transmitters λ_t decreases from 0.6 to 0.2, the optimal value of λ_j needs to be increased to ensure the optimal transmission probability. This is resulting from the fact that transmitters with the lower intensity have less chance to be charged by jammers.

Fig. 5 shows the results of the optimal intensity of jammers λ_j versus transmission power of jammers P_j with different path loss factor α. We can see that the optimal value of λ_j has a decreasing trend with the increased transmission power of jammers, implying that we can use the higher transmission power of jammers to replace the large number of jammers in order to achieve the optimal transmission probability.

In summary, we can achieve the optimal transmission probability by choosing the optimal intensity of jammers according to different channel conditions, node density of transmitters and transmission power of jammers.

VI. Conclusion

In this paper, we propose a new Wireless-Jamming-Energy-Transfer (WJET) scheme by integrating friendly-jamming scheme with wireless energy transfer. In particular, we establish an analytical model to investigate the transmission probability and the eavesdropping probability. The results show that WJET can effectively improve the transmission probability and decrease the eavesdropping probability. In particular, we find that both the transmission probability and the eavesdropping probability heavily depend on the density of jammers and

$$
\begin{aligned}
\frac{\partial \mathbb{P}_t}{\partial \lambda_j} = &\left(\int_0^{\infty} 2r_j e^{-\frac{{r_j}^{\alpha}\theta}{P_j} - {r_j}^2 \pi \lambda_j} \pi - 2{r_j}^3 e^{-\frac{{r_j}^{\alpha}\theta}{P_j} - {r_j}^2 \pi \lambda_j} \pi^2 \lambda_j dr_j \right) \int_0^{\infty} 2e^{-\frac{r^{\alpha}\beta\sigma^2}{P_t} - \pi r^2 \lambda_t \left(\frac{P_j}{P_t}\right)^{2/\alpha} \rho_1 - \pi r^2 \lambda_j \rho_2} \pi r \lambda_t dr + \\
&\left(\int_0^{\infty} 2r_j e^{-\frac{{r_j}^{\alpha}\theta}{P_j} - {r_j}^2 \pi \lambda_j} \pi \lambda_j dr_j \right) \int_0^{\infty} 2e^{-\frac{r^{\alpha}\beta\sigma^2}{P_t} - \pi r^2 \lambda_t \left(\frac{P_j}{P_t}\right)^{2/\alpha} \rho_1 - \pi r^2 \lambda_j \rho_2} - 2e^{-\frac{r^{\alpha}\beta\sigma^2}{P_t} - \pi r^2 \lambda_t \left(\frac{P_j}{P_t}\right)^{2/\alpha} \rho_1 - \pi r^2 \lambda_j \rho_2} \pi^2 r^3 \lambda_t \rho_2 dr.
\end{aligned} \tag{18}
$$

various channel conditions. Extensive simulations verify the effectiveness and the accuracy of our analytical models. Moreover, we extensively achieve the optimal density of jammers in order to have the optimal transmission probability based on various channel conditions, density of transmitters and transmission power of jammers.

Acknowledgement

The work described in this paper was supported by Macao Science and Technology Development Fund under Grant No. 0026/2018/A1, the Science and Technology Planning Project of Guangdong Province (No. 2017A050501035) and the National Natural Science Foundation of China under Grant 6167050421. The authors would like to express their appreciation for Gordon K.-T. Hon for his thoughtful discussions.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] Y. Zou, X. Wang, and W. Shen, "Eavesdropping attack in collaborative wireless networks: Security protocols and intercept behavior," in *Computer Supported Cooperative Work in Design (CSCWD), 2013 IEEE 17th International Conference on*. IEEE, 2013, pp. 704–709.

[3] S. K. Yu, P. Tague, H. Lee, and H. Kim, "A jamming approach to enhance enterprise wi-fi secrecy through spatial access control," *Wireless Networks*, vol. 21, no. 8, pp. 2631–2647, 2015.

[4] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Friendly jamming for wireless secrecy," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–6.

[5] Z. Han and N. Marina, "Physical layer security game: interaction between source, eavesdropper, and friendly jammer," *Eurasip Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 452907, 2010.

[6] M. Adams and V. K. Bhargava, "Using friendly jamming to improve route security and quality in ad hoc networks," in *Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on*. IEEE, 2017, pp. 1–6.

[7] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.

[8] X. Li, H.-N. Dai, Q. Wang, and A. V. Vasilakos, "Ae-shelter: An novel anti-eavesdropping scheme in wireless networks," in *Communications (ICC), 2017 IEEE International Conference on*. IEEE, 2017, pp. 1–6.

[9] X. Li, H.-N. Dai, and H. Wang, "Friendly-jamming: An anti-eavesdropping scheme in wireless networks of things," in *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016, pp. 1–6.

[10] Y. Liu and P. Ning, "Bittrickle: Defending against broadband and high-power reactive jamming attacks," in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 909–917.

[11] L. Pang and Z. Xue, "A novel anti-jamming method in wireless sensor networks: Using artificial noise to actively interfere the intelligent jammer," in *Systems and Informatics (ICSAI), 2017 4th International Conference on*. IEEE, 2017, pp. 954–959.

[12] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming," *Mobile Networks and Applications*, vol. 19, no. 1, pp. 45–60, 2014.

[13] S. Bi, Y. Zeng, and R. Zhang, "Wireless powered communication networks: An overview," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 10–18, 2016.

[14] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4788–4799, 2013.

[15] H. Jabbar, Y. S. Song, and T. T. Jeong, "Rf energy harvesting system and circuits for charging of mobile devices," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 1, pp. 247–253, 2010.

[16] K. Huang and V. K. Lau, "Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 902–912, 2014.

[17] J. Zhang, G. Pan, and H.-M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, 2016.

[18] Y. Fan, X. Liao, and Z. Gao, "Joint energy harvesting and jamming design in secure communication of relay network," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[19] J. F. C.Kingman, *Poission Processes*. Clarendon Press: Oxford, 1993.