Secure Communication with Wireless Powered Friendly Jammers under Multiple Eavesdroppers

Dongxuan He, He Zhou, Hua Wang, and Dewei Yang
Beijing Institute of Technology, China

***Abstract*—In this work, we propose a secure communication scheme, where a source transmits information to the legitimate receiver in the presence of multiple eavesdroppers. To improve the security, single or multiple friendly jammers are deployed to confuse the eavesdroppers. Specifically, we assume that the jammers have to harvest energy from the source, thus we consider a two-phase transmission scheme where the source transmits energy to the jammers first and then transmits information to the legitimate receiver confidentially with the help of the jammers. We first give the expression of the secrecy outage probability, revealing how the secrecy performance depends on the transmission parameter tuple, and then we use the simulated annealing method to obtain the optimal transmission parameter tuple. The simulation results show the superiority of our proposed scheme.**

I. Introduction

Recently, security in wireless networks has been an important issue due to the broadcasting nature of wireless medium. Traditionally, security in wireless communications is achieved through cryptographic techniques applied on upper layers. However, the decentralized modern wireless networks make the generation, distribution, and management of secret keys hard to realize. To address this issue, physical layer security [1] has been proposed as an alternative to cryptographic techniques, since it can achieve the information-theoretic secure communications using the characteristic of the channel.

To improve the secrecy performance in wireless networks, cooperative schemes, such as cooperative relaying [2–4] and cooperative jamming [5–7], have been adopted. The cooperative relaying scheme typically selects the optimal relay to forward the information [2, 3] or uses multiple relays to transmit the signal collaboratively (such as cooperative beamforming [4]). As for the cooperative jamming scheme, friendly jammers are utilized to interfere the eavesdropper to improve the transmission security. For instance, the authors in [5] studied the power minimization and secrecy rate maximization problem in the multiple-input–multiple-output system, where a jammer is used to improve the security. In [6], an optimal jammer selection scheme was proposed to reduce the intercept probability. To optimize the secrecy performance, the optimal deployment of jammer from the geography and time perspective was studied in [7].

Recently, several works studied the wireless powered jammer, where the jammer has to harvest energy from other devices to support its transmission [8–10]. In [8], a secrecy transmission scheme in the orthogonal frequency division multiplexing system was proposed, where a wireless powered jammer is deployed to enhance the transmission security. The author in [9] considered how to maximize the secrecy throughput under the outage constraint with the help of a friendly jammer. However, this paper only analyzed the single eavesdropper situation, and the impact of the fraction of time to the power transfer and information transfer has not been studied. And a secure communication scheme with the help of one energy harvest jammer in the presence of multiple eavesdroppers was studied in [10], while only one jammer was considered to be deployed. In our paper, we consider a more general situation that single or multiple jammers can be deployed in the wireless network in the presence of multiple eavesdroppers.

The contributions of this paper are summarized as follows: 1) We propose a jammer-aided secure communication scheme, where one or multiple jammers use the energy harvested from the source to transmit jamming signal, improving the security of the communication from the source to the legitimate receiver in the presence of multiple eavesdroppers. 2) We give out the expression of the secrecy outage probability, allowing us to explicitly depict the effective secrecy throughput (EST) [11, 12]. 3) Utilizing the simulated annealing (SA) method, we obtain the optimal transmission parameter tuple that maximizes the EST.

II. System Model and Transmission Scheme

As shown in Fig. 1, we consider a secure communication model where a source (Alice) wants to transmit information to a legitimate receiver (Bob) confidentially in the presence of multiple non-colluding eavesdroppers (Eves). To improve the security, we assume a jammer is deployed to confuse the eavesdroppers, and we also assume the jammer has to harvest energy from Alice to support its transmission. In this model, we assume that all the nodes are single antenna nodes.

As for the communication links, we denote the channel between Alice and the jammer, Bob, and the k-th Eve as h_{aj}, h_{ab}, and $h_{ae,k}$, respectively, and we denote the channel between the jammer and Bob and the k-th Eve as g_{jb} and $g_{je.k}$, we assume that all the channels experience identical and independent distributed (i.i.d) Rayleigh fading. As such, we note that the entries of h_{aj}, h_{ab}, $h_{ae,k}$, g_{jb}, and $g_{je.k}$ are complex Gaussian variable with zero mean and unit variance. We also assume that the channel state information (CSI) of h_{aj}, h_{ab}, and g_{jb} is perfectly known to Alice, while only statistical CSI of $h_{ae,k}$ and $g_{je.k}$ is known to Alice.

978-1-7281-1217-6/19/$31.00 ©2019 IEEE

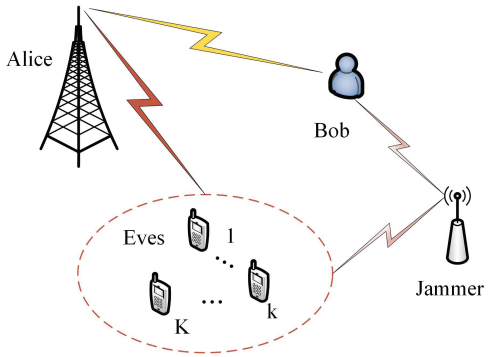

Fig. 1. Illustration of Single Jammer-Aided System Model.

A. Secure Transmission Scheme

We assume the transmission scheme consists of two phases, i.e., the wireless energy transfer (WET) phase and the wireless information transfer (WIT) phase. During the WET phase, Alice transmits energy to the jammer, and the jammer will store all the harvested energy in its battery. We assume the fraction of time allocated to the WET phase is τ, as such, we can formulate the jamming power of the jammer in the WIT phase as

$$P_j = \rho\varphi|h_{aj}|^2 P_a, \tag{1}$$

where $0 < \rho < 1$ is the energy harvest efficiency, $\varphi = \tau/(1-\tau)$, and P_a is the transmit power of Alice.

Then, Alice transmits the confidential information to Bob with the help of jammer. Here, we can formulate the received signal at Bob and the k-th Eve as

$$y_b = \sqrt{P_a}h_{ab}s + \sqrt{P_j}g_{jb}t + n_b, \tag{2}$$

$$y_k = \sqrt{P_a}h_{ae,k}s + \sqrt{P_j}g_{je,k}t + n_k, \tag{3}$$

where n_b and n_k are the thermal noise at Bob and the k-th Eve, which are assumed to be complex Gaussian random variables with zero mean and variance σ_b^2 and σ_k^2, respectively. We assume that $\sigma_k^2 = \sigma_e^2$ for $k = 1, \cdots, K$ in the following analysis. s is the information signal with $\mathbb{E}\left[|s|^2\right] = 1$, t is the jamming signal with $\mathbb{E}\left[|t|^2\right] = 1$. As such, we can formulate the received signal-to-interference-plus-noise ratios (SINRs) at Bob and the k-th Eve as

$$\gamma_b = \frac{P_a|h_{ab}|^2}{P_j|g_{jb}|^2 + \sigma_b^2}, \tag{4}$$

$$\gamma_k = \frac{P_a|h_{ae,k}|^2}{P_j|g_{je,k}|^2 + \sigma_e^2}. \tag{5}$$

According to (4) and (5), the secrecy capacity of our system can be formulated as

$$C_s = \max\left\{C_b - C_e, 0\right\}, \tag{6}$$

where $C_b = \log_2(1+\gamma_b)$ and $C_e = \log_2(1+\gamma_e)$ denote the capacity of the main channel and the wiretap channel, respectively, and $\gamma_e = \max\{\gamma_k\}$, for $k = 1, \cdots, K$, since the eavesdropped information is determined by the maximal SINR of eavesdroppers in the non-colluding eavesdropping mode [13].

B. Problem Formulation

To guarantee the confidentiality of information, we assume the well-known Wyner code with code rate (R_b, R_s) is utilized, where R_b is the transmission rate of the wiretap code and R_s is the secrecy transmission rate. The difference between the transmission rate and the secrecy rate, i.e., $R_b - R_s$, is the redundancy rate against eavesdropping. Once the capacity of the wiretap channel is larger than the redundancy rate, the eavesdropper can decode information from its received signal, so we think that the information is leaked, and secrecy outage occurs. Since we assume that the CSI of the legitimate channel (i.e., h_{ab}, h_{aj}, and g_{jb}) is perfectly known to Alice, we can set $R_b = C_b$. By the reason that the eavesdroppers work in a non-colluding mode, we can define the secrecy outage probability as

$$P_{s,out}(\tau, R_s) = \Pr(\gamma_e > \kappa_e), \tag{7}$$

where $\kappa_e = 2^{R_b - R_s} - 1$.

To evaluate the secrecy performance, we adopt the modified EST [11, 12] as the performance metric, which can be formulated as

$$T_s(\tau, R_s) = (1-\tau)R_s(1 - P_{s,out}(\tau, R_s)). \tag{8}$$

Here, the factor $1-\tau$ is adopted for only $1-\tau$ fraction of time is used for information transmission.

From (8), we can see that the secrecy performance depends on the selection of τ and R_s, as such, the optimization problem is given by

$$\max_{\tau, R_s} \quad T_s(\tau, R_s), \tag{9a}$$

$$\text{s.t.} \quad 0 < \tau < 1, 0 < R_s \le R_b. \tag{9b}$$

In the following, we will show how the transmission parameters will influence the EST and the method to select the transmission parameter tuple.

III. Effective Secrecy Throughput Maximization

In this section, we detail how to maximize the effective secrecy throughput with the help of the jammer. Specifically, we first derive the secrecy outage probability of our system, and then we show the method to find the optimal transmission parameter tuple (τ^*, R_s^*).

A. Secrecy Outage Probability

To calculate the effective secrecy throughput, we first show the secrecy outage probability in the following lemma.

Lemma 1. *The secrecy outage probability when the K eavesdroppers work in a non-colluding mode can be expressed as*

$$P_{s,out}(\tau, R_s) = 1 - \left(1 - \frac{P_a e^{-\frac{\sigma_e^2 \kappa_e}{P_a}}}{\kappa_e P_j + P_a}\right)^K. \tag{10}$$

Proof: The secrecy outage probability is determined by the eavesdropper with the strongest eavesdropping ability. Here, we calculate the cumulative distribution function (CDF) of γ_k first. With the aid of (5), we can express the CDF of γ_k as

$$\begin{aligned} F_{\gamma_k}(z) &= \Pr\left(\frac{P_a|h_{ae,k}|^2}{P_j|g_{je,k}|^2+\sigma_e^2} \le z\right) \\ &= \Pr\left(|h_{ae,k}|^2 \le \frac{P_j|g_{je,k}|^2+\sigma_e^2}{P_a z^{-1}}\right) \\ &= \int_0^\infty F_{|h_{ae,k}|^2}\left(\frac{P_j x+\sigma_e^2}{P_a z^{-1}}\right) f_{|g_{je,k}|^2}(x)\,dx. \end{aligned} \tag{11}$$

Now, we focus on the CDF of $|h_{ae,k}|^2$ and the probability density function (PDF) of $|g_{je,k}|^2$. For all the channels subject to the i.i.d Rayleigh fading. Hence, we have $|h_{ae,k}|^2 \sim \exp(1)$, and the CDF of $|h_{ae,k}|^2$ can be expressed as

$$F_{|h_{ae,k}|^2}(x) = 1 - e^{-x}. \tag{12}$$

Besides, we also note that $|g_{je,k}|^2 \sim \exp(1)$. To this end, we can express the PDF of $|g_{je,k}|^2$ as

$$f_{|g_{je,k}|^2}(x) = e^{-x}. \tag{13}$$

Substituting (12) and (13) into (11), we obtain the closed-form expression of the CDF of γ_k as

$$\begin{aligned} F_{\gamma_k}(z) &= \int_0^\infty \left(1-\exp\left(-\frac{P_j x+\sigma_e^2}{P_a z^{-1}}\right)\right)\exp(-x)\,dx \\ &= 1 - \frac{P_a e^{-\frac{\sigma_e^2 z}{P_a}}}{zP_j+P_a}. \end{aligned} \tag{14}$$

As mentioned before, we assume that all the Eves work in a non-colluding mode, thus we can express the CDF of γ_e as

$$F_{\gamma_e}(z) = (F_{\gamma_k}(z))^K = \left(1 - \frac{P_a e^{-\frac{\sigma_e^2 z}{P_a}}}{zP_j+P_a}\right)^K. \tag{15}$$

With the help of (7) and (15), we can obtain the closed-form expression of the secrecy outage probability as

$$\begin{aligned} P_{s,out}(\tau, R_e) &= 1 - \Pr(\gamma_e \le \kappa_e) \\ &= 1 - \left(1 - \frac{P_a e^{-\frac{\sigma_e^2 \kappa_e}{P_a}}}{\kappa_e P_j + P_a}\right)^K. \end{aligned} \tag{16}$$

The proof is completed. ∎

B. Transmission Parameters Design

Substituting the expression of secrecy outage probability into (8), we can find this problem is hard to solve directly due to the complicated expression of the objective function of problem (9). Besides, the numerical approach is not suitable for this problem for problem (9) is a continuous optimization problem.

To solve this problem, we consider to utilize the simulated annealing algorithm to find the solution. The SA method is a probabilistic optimization method which does not concern the expression of this problem, and this method finds the solution through iterative searching. Specifically, the SA method can approximate the global optimization in a large search space, avoiding getting stuck in the local optimum points [14].

To be noticed, the two transmission parameters are coupled, the constraint (9b) requires that $R_s \le R_b$. To this end, we first generate the time allocation fraction, and then we generate a R_s that satisfies the constraint. To show how to utilize the SA method to determine the optimal transmission parameter tuple, we present the details in **Algorithm** 1.

Algorithm 1 SA method to determine the optimal transmission parameter tuple.

1: Initialize: initial temperature T, temperature reducing factor α.
2: Randomly generate a time allocation fraction τ_0 and $R_{s,0}$ satisfying $R_{s,0} \le R_{b,0}$, calculate the $T_{s,0}$ (i.e., $E(\tau_0, R_{s,0})$) using (8) and (16).
3: **while** $T > T_{min}$ **do**
4: Randomly generate a time allocation fraction τ_1 and $R_{s,1}$ satisfying $R_{s,1} \le R_{b,1}$, calculate the $T_{s,1}$ (i.e., $E(\tau_1, R_{s,1})$).
5: $\Delta E = E(\tau_0, R_{s,0}) - E(\tau_1, R_{s,1})$.
6: **if** $\Delta E < 0$ **then**
7: Update τ_0, $R_{s,0}$, and $E(\tau_0, R_{s,0})$.
8: **else**
9: **if** $e^{-\frac{\Delta E}{T}} > rand[0,1]$ **then**
10: Update τ_0, $R_{s,0}$, and $E(\tau_0, R_{s,0})$.
11: **end if**
12: **end if**
13: $T = \alpha T$
14: **end while**

IV. Multiple Friendly Jammers-Aided Secure Transmission

In the above analysis, only one friendly jammer is assumed to be deployed. Now, we further consider the situation that M friendly jammers are utilized to enhance the security. As such, we first express the jamming power of the m-th jammer as

$$P_{j,m} = \rho\varphi|h_{aj,m}|^2 P_a, \tag{17}$$

where $h_{aj,m}$ is the channel between Alice and the m-th jammer.

Here, we can re-express the SINRs of Bob and the k-th eavesdroppers as

$$\gamma_b = \frac{P_a|h_{ab}|^2}{\sum_{m=1}^M P_{j,m}|g_{jb,m}|^2+\sigma_n^2}, \tag{18}$$

$$\gamma_k = \frac{P_a|h_{ae,k}|^2}{\sum_{m=1}^M P_{j,m}|g_{je,mk}|^2+\sigma_k^2}, \tag{19}$$

where $g_{jb,m}$ and $g_{je,mk}$ are the channel from the m-th jammer to Bob and the k-th eavesdropper, respectively.

And then, we give out the secrecy outage probability for the multiple jammers-aided secure transmission, which can be expressed as

$$P_{s,out}(\tau, R_s) = 1 - \left(\int_0^{\infty} F_{|h_{ae,k}|^2} \left(\frac{x + \sigma_e^2}{P_a \kappa_e^{-1}} \right) f_\gamma(x)\, dx \right)^K, \tag{20}$$

where $f_\gamma(\cdot)$ is the PDF of $\sum_{m=1}^{M} P_{j,m} |g_{je,mk}|^2$. Suppose that L jammers has the same jamming power $P_0 = 1/\lambda_0$, and the left $N = M - L$ jammers have different jamming power $P_n = 1/\lambda_n$, where $n = 1, \cdots, N$, then we can express $f_\gamma(\cdot)$ as [15]

$$f_\gamma(\gamma) = \left(\sum_{n=1}^{N} E_n \lambda_n \exp(-\lambda_n \gamma) + \sum_{l=1}^{L} A_l \frac{\gamma^{l-1} \lambda_0^l \exp(-\lambda_0 \gamma)}{\Gamma(l)} \right) U(\gamma). \tag{21}$$

In (21), $U(\gamma)$ is a unit step function, and $\Gamma(\cdot)$ is the Gamma function, defined as [16, eq. (8.310)]

$$\Gamma(z) = \int_0^{\infty} \exp(-t)\, t^{z-1} dt, \tag{22}$$

Besides, the other parameters in (21) can be respectively expressed as

$$E_n = \left(\frac{1}{1 - \lambda_n/\lambda_0} \right)^L \prod_{u=1, u \neq n}^{N} \frac{1}{1 - \lambda_n/\lambda_u}, \tag{23}$$

$$C_{u,v} = \frac{1}{(1 - B_u/\lambda_0)^v}, \tag{24}$$

$$D_u = \left(\frac{1}{1 - B_u/\lambda_0} \right)^L \prod_{n=1}^{N} \frac{1}{1 - B_u/\lambda_n} - \sum_{n=1}^{N} \frac{E_n}{1 - B_u/\lambda_n}, \tag{25}$$

where $\{C_{u,v}\}$ is the element of a $L \times L$ matrix $\boldsymbol{C}$, $\{D_u\}$ is the element of a $L \times 1$ matrix $\boldsymbol{D}$, and $\boldsymbol{A} = \boldsymbol{C}^{-1} \times \boldsymbol{D}$. In addition, B_p, where $p = 1, \cdots, L$, can be obtained from the following equation

$$\left(1 - \frac{B_p}{\lambda_0}\right)^{-L} \prod_{n=1}^{N} \left(1 - \frac{B_p}{\lambda_n}\right)^{-1} = \sum_{n=1}^{N} E_n \left(1 - \frac{B_p}{\lambda_n}\right)^{-1} + \sum_{l=1}^{L} A_l \left(1 - \frac{B_p}{\lambda_0}\right)^{-l}, \tag{26}$$

Substituting (20) into (8), we can obtain the EST of the multiple jammers-aided scheme, where the EST is also determined by the transmission parameter tuple (τ, R_s). Analogously, we can utilize the SA method to find the optimal transmission parameter tuple, which has been show in **Algorithm** 1.

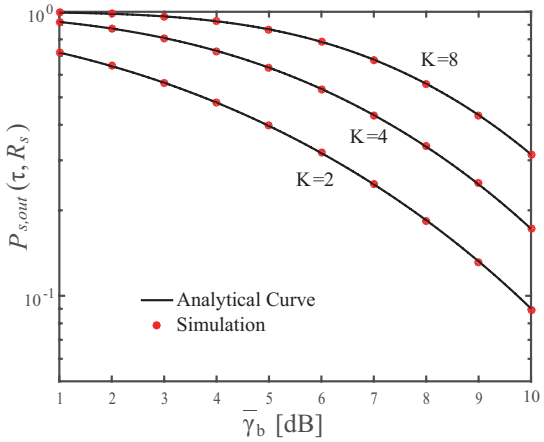

Fig. 2. $P_{s,out}(\tau, R_s)$ versus $\overline{\gamma}_b$ for different values of K with $M = 1$, $\overline{\gamma}_e = 10$ dB, $\tau = 0.6$, and $R_s = 0.1$ bits/s/Hz.

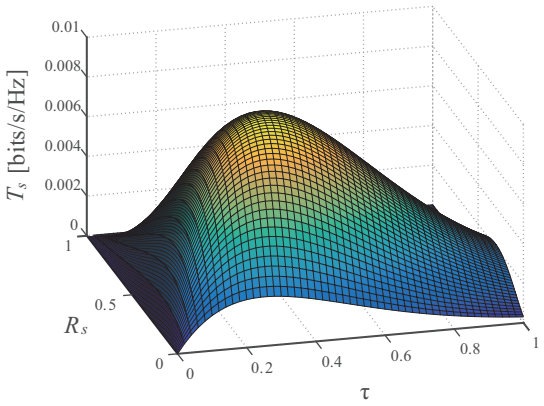

Fig. 3. $T_s(\tau, R_s)$ versus τ and R_s with $M = 1$, $K = 4$, $\overline{\gamma}_b = 10$ dB, and $\overline{\gamma}_e = 10$ dB.

V. Numerical Results

In this section, we present numerical results to validate our analysis. Specifically, we first demonstrate the accuracy of the closed-form expression of the secrecy outage probability. And then, we show how the selection of the transmission parameter tuple will influence the achieved EST. At last, we will show the effectiveness of our proposed algorithm. Specifically, we define $\overline{\gamma}_b = P_a/\sigma_b^2$ and $\overline{\gamma}_e = P_a/\sigma_e^2$.

We first verify the accuracy of the expression of the secrecy outage probability in Fig. 2, which plots $P_{s,out}(\tau, R_s)$ versus $\overline{\gamma}_b$ for different values of K with $M = 1$, $\overline{\gamma}_e = 10$ dB, $\tau = 0.6$, and $R_s = 0.1$ bits/s/Hz. We can see that the simulation points match with the analytical curve, which validates our derivation. And we also find that $P_{s,out}(\tau, R_s)$ increases as the increase of the number of eavesdroppers. In addition, the secrecy outage probability decreases as the increase of $\overline{\gamma}_b$.

In Fig. 3, we plot the effective secrecy throughput versus the transmission parameters. We can see that the EST first increases and then decreases as the increase of τ for any value of R_s. And the similar tendency can be observed from

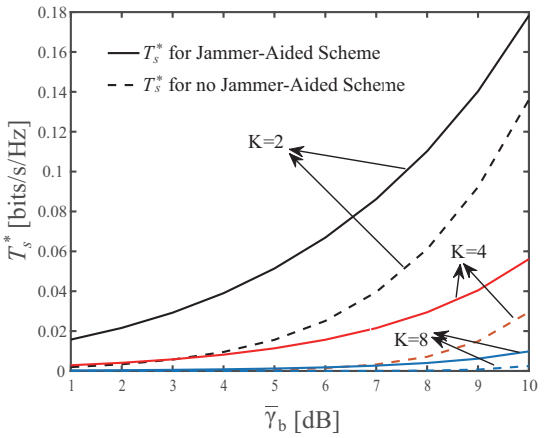

Fig. 4. T_s^* versus $\overline{\gamma}_b$ for different values of K with $M = 1$, $\overline{\gamma}_e = 10$ dB.

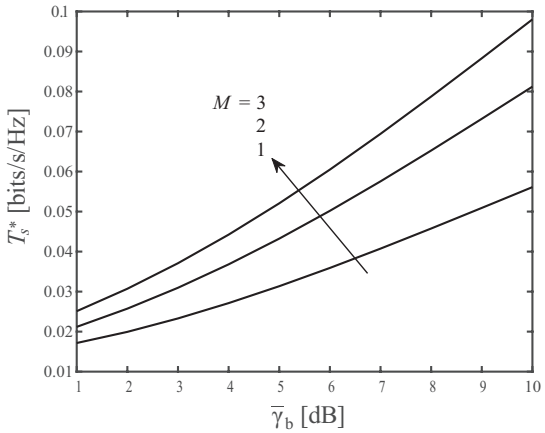

Fig. 5. T_s^* versus $\overline{\gamma}_b$ for different values of M with $\overline{\gamma}_e = 10$ dB, and $K = 4$.

the impact of R_s on T_s. This observation demonstrates that there exists a unique transmission parameter tuple (τ^*, R_s^*) that maximizes the EST.

Then, we plot the T_s^* achieved by different schemes. In this figure, both the transmission parameter tuples of the jammer-aided scheme and no jammer-aided scheme are obtained by the SA method. We can see from Fig. 4 that the secrecy performance of the jammer-aided scheme is better than that of the no jammer-aided scheme for any configurations. As such, we can improve the secrecy performance by deploying a friendly jammer. Even though the T_s^* will decrease significantly as the increase of the number of eavesdroppers, deploying a jammer is always helpful to improve the secrecy performance of our considered system.

At last, we plot T_s^* versus $\overline{\gamma}_b$ for different values of M in Fig. 5. We can see from this figure that the achieved optimal EST increases as the increase of M, because deploying more jammers can achieve the same strength of interference while spending less time in the WET phase.

VI. Conclusion

In this paper, we investigated a secure communication scheme that Alice communicates with Bob in the presence of multiple eavesdroppers. In this scheme, we considered single or multiple wireless powered friendly jammers are deployed to confuse the eavesdroppers. The proposed scheme consists of two phases, Alice first transmits energy to the jammer in the first phase and then transmits information to Bob in the second phase. We demonstrated how our proposed scheme can increase the effective secrecy throughput by judiciously selecting the transmission parameter tuple, and then we utilized the simulated annealing method to obtain the optimal transmission parameter tuple. And our simulation results showed the superiority of the jammer-aided scheme compared to the no jammer-aided scheme.

VII. Acknowledgement

This work was supported by the National Natural Science Foundation of China under Grant No. 61471037, No. 61771048, and No. 61201181.

References

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[2] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[3] F. S.-A. Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756–1770, May 2015.

[4] M. Lin, J. Ge, Y. Yang, and Y. Ji, "Joint cooperative beamforming and artificial noise design for secrecy sum rate maximization in two-way AF relay networks," *IEEE Commun. Lett.*, vol. 18, no. 2, pp. 380–383, Feb. 2014.

[5] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[6] H. Huang, X. Zhang, X. Hu, P. Zhang, and Y. Li, "An optimal jammer selection for improving physical-layer security in wireless networks with multiple jammers," *in Proc. Int. Wireless Commun. Mobile Comput. Conf.*, Sep. 2016, pp. 719–724.

[7] Y. Allouche et al., "Secure Communication through Jammers Jointly Optimized in Geography and Time," *ACM MobiHoc*, Hangzhou, China, June 2015, pp. 227–236.

[8] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative jamming for secure OFDM system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1331–1346, Feb. 2018.

[9] W. Liu, X. Zhou, S. Durrani, and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401–415, Jan. 2016.

[10] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 764–774, Feb. 2017.

[11] C. Liu, N. Yang, J. Yuan, and R. Malaney, "Location-based secure transmission for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 7, pp. 1458–1470, Jul. 2015.

[12] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[13] W. Wang, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Security.*, vol. 12, no. 3, pp. 505–515, Mar. 2017.

[14] D. Bertsimas and J. Tsitsiklis, "Simulated annealing," *Statist. Sci.*, vol. 8, no. 1, pp. 10–15, 1993.

[15] H. V. Khuong and H. Y. Kong, "General expression for pdf of a sum of independent exponential random variables," *IEEE Commun. Lett.*, vol. 10, no. 3, pp. 159–161, Mar. 2006.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Tabel of Integrals, Series, and Products,* 7th ed. New York, NY, USA: Academic, 2007.