2019 IEEE International Workshop on Signal Processing Systems

On Secrecy Energy Efficiency of RF Energy Harvesting System

Zhengxia Ji[1], Mengyun Nie[1], Lingquan Meng[1], Qingran Wang[1], Chunguo Li[2,3], Kang Song[1,2,*]
[1] School of Electronic and Information Engineering, Qingdao University, Qingdao 266071, China
[2] School of Information Science and Engineering, Southeast University, Nanjing 210096, China
[3] School of Information Engineering, Xizang Minzu University, Xianyang 712082, China
[*] Email: sk@qdu.edu.cn

***Abstract*—The increasing use of information source in unreliable wireless communication is a driving force to explore the networks' energy efficiency and security. To fully improve the performance of the system, in this paper, we combine these two directions and investigate the secrecy energy efficiency (SEE) of the network in which the information can be eavesdropped consisting of an energy source, an information source, a destination and an eavesdrop node, all of which are equipped with single antenna. The system model is based on ST (save-then-transmit) protocol. The information source node harvests energy from the received signal power to charge its battery, which is used to retransmit the received signal to the destination. Under the limited transmit power mode, we get the expression for SEE, which depends on energy absorption rate and time. Our analytical results reveal that the secrecy efficiency has a maximum. The optimal energy absorption rate was further calculated by Newton iterative algorithm. Then we propose optimal energy source selection method. Simulation results finally verify the accuracy and efficiency of our proposed algorithm for secrecy energy efficiency maximization.**

***Index Terms*—Gaussian wiretap channel, secrecy energy efficiency, ST(Save-then-Transmit), RF energy harvesting**

I. INTRODUCTION

With the rapid development of wireless communication network and the increasing number of mobile terminal users [1], the era of internet has come, and the role of relay in communication has become obviously significant [2]. However, in the past, the relays were all powered by batteries, which would be costly to replace in special circumstances. Moreover, the battery life was limited and had great limitations [3]. In [4], the energy harvesting model was established and the feasibility of energy collection was confirmed, meanwhile the authors proposed various effective energy collection plans. There are many energy sources for energy collection, such as solar energy, wind energy, etc, but such sources are not controllable. A cognitive radio (CR) system based on energy acquisition was analyzed in [5], which is powered by a stable energy source from a single user (PU) radio frequency (RF) signal in the sensing time. The communication system that can transmit information and energy simultaneously has attracted extensive attention in the industry. Aiming at this topic, a scheme of interference auxiliary energy acquisition of cooperative relay system was proposed in [6], where the energy-limited relay obtains energy from the received information signal and co-channel interference signal.

Wireless communication brings convenience to people, but also accompanied by great security risks at the same time. Because of the broadcast and openness of the wireless channel, the eavesdropper can take advantage of it. Many researchers have put forward different countermeasures. From the view of physical layer security, the high-efficiency, energy-saving and secrecy communication based on untrusted two-hop relay were considered in [7], so as to prevent the eavesdropper from intercepting the user's confidential information. Several examples of network were given in [8], in which secrecy physical layer network coding realized a high system performance that cannot be realized by secrecy network coding. In view of these two directions, many people had carried out joint optimization methods. H. J. Visser and R. J. M. Vullers presented an overview of principles and requirements for powering wireless sensors by RF energy harvesting or transport in [9]. The feasibility of harvesting was also discussed, leading to the conclusion that RF energy transport was preferred for powering small sized sensors. Based on the relation of secrecy capacity in wireless eavesdropping channel, the formula of secrecy rate was obtained in [10]. Aimed at the maximum secrecy efficiency different models were established according to energy collection time and energy absorption rate which were all optimized in [11], [12] under certain constraints. In [13], it studied joint beamforming optimization for the wireless powered MP-TWRN in the relaying system under both the amplify-and-forward (AF) and decode-and-forward (DF) relaying mode. But the impact of circuits consumption was ignored. In [14], a large scale multiple input multiple output (LS-MIMO) relaying system was considered where an information source sends the message to its intended destination aided by a LS-MIMO relay, while a passive eavesdropper tried to intercept the information forwarded by the relay. However, the source transmit information only, so the energy efficiency was not considered. In [15], A. Salem, K. A. Hamdi and K. M. Rabie analyzed the secrecy capacity of a half-duplex energy harvesting based multi-antenna amplify-and-forward relay network in the existence of a passive eavesdropper. It's original that the legitimate destination transmits an auxiliary artificial noise (AN) signal to transfer power to the relay and to improve system security.

In [16], a novel cooperative jamming approach was proposed in a multiple-input single-output (MISO) wiretap chan-

978-1-7281-1927-4/19/$31.00 ©2019 IEEE

nel, which sent the Gaussian noise signal by a friendly jammer to disrupt the reception of the eavesdropper and improved the legitimate reception. In [17], the energy efficiency (EE) of wireless energy harvesting power-splitting-based system has been studied. And the author proved it feasible to optimize the number of the antennas.

In this paper, firstly, we propose an energy-harvesting Gaussian eavesdropping channel based on ST (save-then-transmit) protocol. Secondly, considering the security and energy limitation of wireless systems, this paper analyses the problem of maximizing secrecy energy efficiency. To improve system performance, we propose optimal energy source selection method. Thirdly, the method of solving the optimal solution of energy efficiency is given. Finally, the feasibility of the proposed scheme is verified by numerical results, and the influence of energy absorption rate and energy harvesting time on secrecy energy efficiency are studied by control variable method. And then we extend and evaluate the research model.

The remainder of this article is distributed as follows: In section II, we describe the specific model of the system and the associated variables. In section III, the problem of maximizing secrecy energy efficiency has been raised, and introduces the specific steps to solve the optimization problem, namely, maximizing secrecy energy efficiency. Then we proposed the method of optimal energy source selection in section IV. Numerical results and simulation figures are presented in section V to verify the effectiveness of the proposed structure. Finally, conclusions are given in section VI.

II. System Model

In this paper, we consider a generic wireless sensor network based on ST system, which consists of an energy source, an information source, a destination and an eavesdrop node as depicted in Fig. 1. Each device within the network is equipped with single antenna. Due to the limitation of transmit power and actual communication distance, there is no direct link between the energy source and the destination. The information source contains an energy harvester, and operates in a half-duplex mode, where the total transmit time T is divided into different parts.

We assume that the system channel is Rayleigh fading channel, in which the channel coefficients have independent and identical distribution and remain constant within a transmit process. It is assumed that there is perfect channel state information (CSI) for all transmissions known at the destination node. Fig. 2 shows the time-sharing allocation convention in ST scheme: i) energy transmission from the energy source to information source, ii) message forwarding from information source to the destination. The link between the energy source and information source is active for two fractions: βT seconds used for energy transmitting while the link between the information source and destination is active for the remaining $(1-\beta)T$ for information transmitting, where $0 \leq \beta \leq 1$. Furthermore, we assume that the energy harvesting at the information source takes up so little time that can be ignored. To simplify the formula, we adopt normalized time without loss in generality.

We define that x_1 is the normalized information signal at x_1 with $E\{|x_1|^2\} = 1$. Let h, g_D and g_E denotes the channel coefficients in the energy source-information source link, information source-destination link and information source-eavesdropper link, respectively. And we assume that the information source only retransmit confidential information to the destination when the eavesdropping channel is worse than $S - D$ link, that is to say $|g_D| > |g_E|$. What's more, P_S and P_R denotes the transmit power at the energy source and information source respectively.

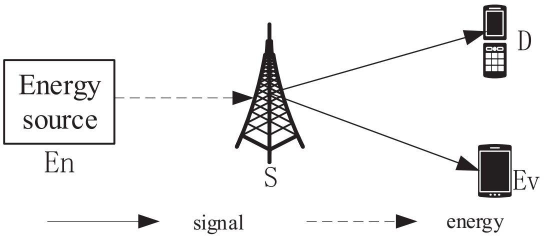

Fig. 1. The system model.

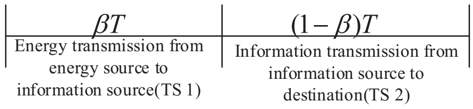
βT
$(1-\beta)T$
Energy transmission from energy source to information source(TS 1)
Information transmission from information source to destination(TS 2)

Fig. 2. ST protocol model.

III. Optimization of Secrecy Energy Efficiency

In the first phase, the signal is transmitted from E_n to S. The received signal at the information source node can be expressed as

$$y_R = \sqrt{P_S} h x_1 + n_1 \tag{1}$$

where x_1 is the normalized information signal at S. n_1 is the additive white Gaussian noise (AWGN) at the information source end, which is an independent and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and unit variance σ_1^2.

Simultaneously, the information source harvest energy come from the energy source. Then in the second phase information source uses the energy to transmit information to D. The signal received at the destination or the eavesdropping end can be given by

$$y_{\mathrm{j}} = \sqrt{P_R} g_j x_2 + n_j \qquad j \in (D, E) \tag{2}$$

where n_j is the additive white Gaussian noise (AWGN) at the destination and eavesdropping end, which is an independent and identically distributed (i.i.d.) complex Gaussian random variable with zero mean and variance σ_j^2 which is considered as unit variance. g_D and g_E are the channel coefficient of the primary channel and the eavesdropping channel, respectively.

According to the ST protocol, in this model, βT part of the total time is used to absorb energy, and the rest of the time is used for data transmission. So the total energy absorbed by information source can be expressed by

$$Q = v_s \beta T = \xi P_S |h|^2 \beta T \tag{3}$$

where v_s denotes energy absorption rate, and it satisfies the limit of maximum energy absorption rate which can represent as $0 < v_s < v_{max}$. And ξ represents the energy harvesting coefficient. And it can be obtained by equation (3)

$$P_S = \frac{v_s}{\xi |h|^2} \tag{4}$$

Assuming that the transmission equipment uses the average power supply, the average power of the information source during the data transmission satisfies

$$P_R = \frac{v_s \beta T}{(1-\beta)T} = \frac{v_s \beta}{(1-\beta)} \tag{5}$$

From [2], we can get the expression of secrecy rate of the system

$$R_S = (1-\beta)\log_2 \frac{1-\beta+\beta v_s |g_D|^2}{1-\beta+\beta v_s |g_E|^2} \tag{6}$$

The total power consumption for the system can be given by

$$P_{total} = P_C + P_S \tag{7}$$

where P_C is the total circuits consumption.

The secrecy energy efficiency of the model is defined as

$$U(P_S, \beta) = \frac{R_S}{P_{total}} \tag{8}$$

A. Optimization for v_s

In this section, we investigate the variation of secrecy energy efficiency with the equivalent energy absorption rate at the transmitter.

The secrecy energy efficiency of the system can be expressed as

$$U = \frac{R_S}{P_C + P_{\mathrm{S}}} = \frac{(1-\beta)\log_2 \frac{1-\beta+\beta v_s |g_D|^2}{1-\beta+\beta v_s |g_E|^2}}{\frac{v_s}{\xi |h|^2} + P_C} \tag{9}$$

According to equation (4), P_S and v_s have a linear relationship, so $U(P_S, \beta) = U(v_s, \beta)$. Accordingly, the resource allocation under secrecy energy efficiency optimization could be formulated as

$$\begin{aligned} & \max U(v_s, \beta) \\ s.t. \quad & 0 < \beta < 1 \\ & 0 < v_{\mathrm{s}} < v_{\max} \end{aligned} \tag{10}$$

Theorem 1: There exists $v_s = v_s^*$ belongs to $(0, v_{\max})$ that can make U reaching the maximum, and v_s^* is unique.

Proof: The first order derivative of U is

$$\begin{aligned} \frac{\partial U}{\partial v_s} = & \frac{\xi |h|^2 (1-\beta)}{(v_s + \xi |h|^2 P_C)^2} [(\frac{\beta |g_D|^2}{1-\beta+\beta v_s |g_D|^2} \\ & - \frac{\beta |g_E|^2}{1-\beta+\beta v_s |g_E|^2})(\frac{v_s + \xi |g_E|^2 P_C}{\ln 2}) \\ & -\log_2(1-\beta+\beta v_s |g_D|^2) + \log_2(1-\beta+\beta v_s |g_E|^2)] \end{aligned} \tag{11}$$

With the fact that $\frac{\xi |h|^2 (1-\beta)}{(v_s+\xi |h|^2 P_C)^2} > 0$, it is clear that the numerator has the same sign as $\frac{\partial U}{\partial v_s}$. We define

$$\begin{aligned} M = & \left(\frac{\beta |g_D|^2}{1-\beta+\beta v_s |\mathrm{g}_D|^2} - \frac{\beta |g_E|^2}{1-\beta+\beta v_s |g_E|^2} \right) (\frac{v_s + \xi |h|^2 P_c}{\ln 2}) \\ & -\log_2(1-\beta+\beta v_s |g_D|^2) + \log_2(1-\beta+\beta v_s |g_E|^2) \end{aligned} \tag{12}$$

The first order derivative of M is

$$\frac{\partial M}{\partial v_s} = (v_s + \xi |h|^2 P_C)[\frac{(\beta |g_E|^2)^2}{(1-\beta+\beta v_s |g_E|^2)^2} - \frac{(\beta |g_D|^2)^2}{(1-\beta+\beta v_s |g_D|^2)^2}] \tag{13}$$

That is

$$\frac{\partial M}{\partial v_s} = (v_s + \xi |h|^2 P_C)[\frac{\beta^2}{(\frac{1-\beta}{|g_E|^2}+\beta v_s)^2} - \frac{\beta^2}{(\frac{1-\beta}{|g_D|^2}+\beta v_s)^2}] \tag{14}$$

Since $M' < 0$ is always true, M is a decrease function, and

$$\begin{cases} \lim\limits_{x \to 0} M = \frac{\beta |g_D|^2 (1 - \frac{|g_E|^2}{|g_D|^2})}{1-\beta} (\frac{vs + \xi |h|^2 P_C}{\ln 2}) > 0 \\ \lim\limits_{x \to \infty} M = \frac{|g_E|^2 - |g_D|^2}{\beta |g_D|^2 |g_E|^2 \ln 2} + \log_2 \frac{|g_E|^2}{|g_D|^2} < 0 \end{cases} \tag{15}$$

It is clear that the function U increases at first and then decreases. Therefore, it can be known from theorem one that there exists only one v_s that makes U largest.

B. Optimization for β

In this section, we discussed the optimal energy harvesting time β. We take the derivative of the target function in equation (9), with respect to energy harvesting time β.

$$\frac{\partial^2 U}{\partial \beta^2} = \frac{v_s |g_D|^2 (\frac{|g_E|^2}{|g_D|^2} - 1)(v_s |g_D|^2 (1-\beta)(1 + \frac{|g_E|^2}{|g_D|^2}) + 2\beta v_s^2 |g_E|^2)}{(\ln 2)(1-\beta+\beta v_s |g_D|^2)^2 (1-\beta+\beta v_s |g_E|)^2 (\frac{v_s}{\xi |h|^2} + P_C)} \tag{16}$$

when $\frac{|g_E|^2}{|g_D|^2} < 1$ and $\frac{\partial^2 U}{\partial \beta^2} < 0$, U is a convex function. Therefore, the optimal energy absorption rate can be obtained by convex optimization algorithm .

Next, we discuss the optimal solution of energy efficiency by Newton iteration method. Take the first derivation of secrecy energy efficiency with respect to energy harvesting time and energy absorption rate, and we can get $f = \frac{\partial U}{\partial \beta}$ and $g = \frac{\partial U}{\partial v_s}$ respectively. We further define

$$\begin{cases} f_{vs} = \frac{\partial f}{\partial v_s} & f_\beta = \frac{\partial f}{\partial \beta} \\ g_{vs} = \frac{\partial g}{\partial v_s} & g_\beta = \frac{\partial g}{\partial \beta} \end{cases} \tag{17}$$

Since we have proved that the objective function U is convex, Newton iteration method can be adopted here to solve the original optimization problem, as shown in Algorithm 1.

Algorithm 1 Newton iterative algorithm for finding roots of binary equations.

```
$(\beta_1, v_{s_1})$ is arbitrarily chosen from $\beta_1 \in (0,1), v_{s1} \in (0, v_{smax})$
$k = 1$
while $|\max\{f(\beta_k, v_{sk}), g(\beta_k, v_{sk})\}| > \delta$ do
    $\beta_{k+1} = \beta_k + \frac{fg_{vs} - gf_{vs}|_{(\beta_k, v_{sk})}}{g_\beta f_{vs} - f_\beta g_{vs}|_{(\beta_k, v_{sk})}}$
    $v_{s(k+1)} = v_{sk} + \frac{gf_\beta - fg_\beta|_{(\beta_k, v_{sk})}}{g_\beta f_{vs} - f_\beta g_{vs}|_{(\beta_k, v_{sk})}}$
    $k = k + 1$
end while
return $(\beta_k^*, v_{sk}^*)$
```

In Algorithm 1, the optimal energy absorption rate has been calculated by Newton iterative algorithm, where δ is the algorithm terminated threshold δ, as $\delta = 10^{-3}$ and k denotes the number of iterations.

IV. MULTIPLE ENERGY SOURCES WITH ENERGY SOURCE SELECTION

In this section, we propose the best energy source selection method to select the best energy source from several energy sources in single energy source selection scheme based on our derived secrecy energy efficiency described in Section III. To find the solution of this problem, the secrecy energy efficiency is calculated for each information source while v_s and β are considered as constant. Then the energy source with the largest SEE is chosen as the optimal one. The system consists of k energy sources , an information sources, a destination and an eavesdropper.

The energy source sends energy to information source in time slot 1 (TS 1). Then in time slot 2 (TS 2), information source sends information to the target node, as depicted in Fig. 3.

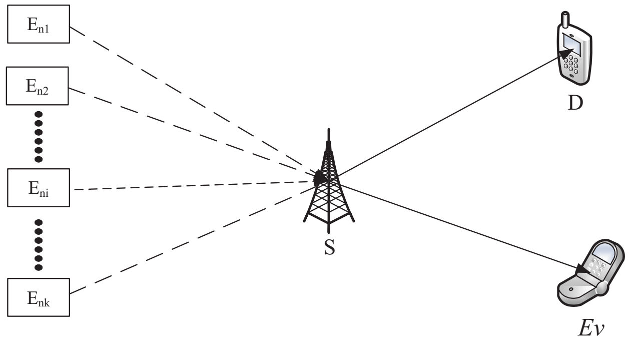

Fig. 3. The system model of information source selection

The secure energy efficiency for the m-th information source can be given by

$$U_{\mathrm{m}} = \frac{R_S}{P_C + P_S} = \frac{(1-\beta)\log_2 \frac{1-\beta+\beta v_s |g_D|^2}{1-\beta+\beta v_s |g_E|^2}}{\frac{v_s}{\xi |h_m|^2} + P_C} \quad (18)$$

$$\forall m = 1, 2, 3.......k$$

Then the best energy source selection is processed, with taking the highest SEE value, which is expressed as

$$\max U_m \ : \forall m \in 1, 2....k \quad (19)$$

The algorithm of energy source selection can be seen from Algorithm 2.

Algorithm 2 The algorithm of optimal information source selection.

```
for each energy source $m = 1 : k$ do
    Calculate Secrecy Energy Efficiency of the m-th energy source
    $U_{\mathrm{m}} = \frac{R_S}{P_C + P_S}$
end for
Find the maximum of $U_m^* = [U_1, U_2, U_3, U_4, ......, U_k]$
return $U_m^*$
```

V. SIMULATION RESULTS

In this section, we provide simulation results to demonstrate the performance of the system based on secrecy energy efficiency with ST. In our simulations, the value of $|\mathrm{g}_D|^2$, $|\mathrm{g}_E|^2$, P_C, ξ and $|h|^2$ has been listed in Table 1.

TABLE I
TABLE OF SIMULATION PARAMETERS

Symbol	*Coefficient*	*Symbol*	*Coefficient*
$\|g_D\|^2$	0.8	$\|g_E\|^2$	0.6
P_C	0.7	ξ	0.84
$\|h\|^2$	0.7		

In order to verify the correctness of the above method, we use genetic algorithm to obtain the maximum value of the target binary function.

In each generation of genetic population, the fitness function is used to judge the individual. The fitness function in this algorithm is proportional to the size of the objective function value. In the genetic process of the next generation, the pre-genetic generation is selected by roulette, that is, the variable with good fitness is more likely to be genetically mutated to the next generation, and the individual with lower fitness also has the opportunity to enter the next generation. The algorithm successfully obtains the maximum value of the function when iterating 100 times.

Fig. 4 shows the secrecy energy efficiency as a function of the energy absorption rate and energy harvesting time. Those points in the figure represents the maximum value at each iteration.

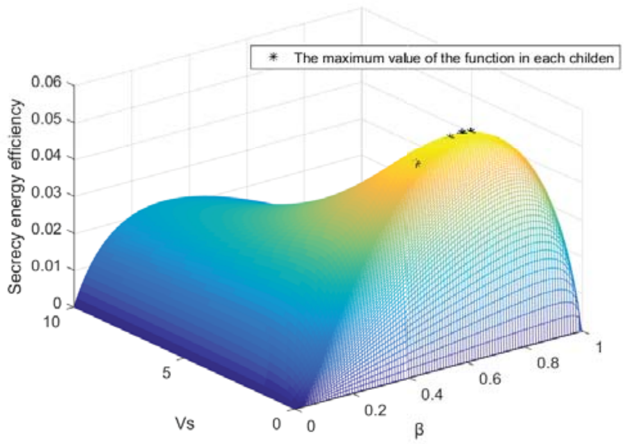

Fig. 4. Relationship between secrecy energy efficiency and energy absorption rate and energy harvesting time

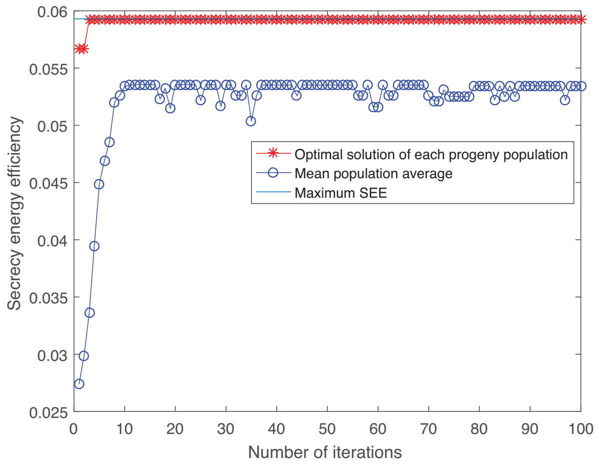

Fig. 5. The relation between the optimal solution and the number of iterations.

Fig 5 shows the relationship between Secrecy energy efficiency and the number of iterations in genetic algorithm. As the number of iterations adds, the number chosen to inherit is more and more proposed, thus the overall fitness of the population becomes better and better and tends to a stable value, and the function value of each child tends to be stable.

Fig. 6 shows the secrecy energy efficiency as a function of the energy absorption rate and energy harvesting time when energy absorption rate changes continuously. It's obviously that there always exists a v_s^* to make U largest with respected to different β, and the maximum of U and v_s^* changes with β. Under the parameters cited in this simulation, we can justice that $\beta^* = 0.6303$ calculated is the optimal value that makes SEE the largest.

Fig. 7 shows the secrecy energy efficiency as a function of the energy absorption rate and energy harvesting time when energy absorption rate changes continuously. It's obviously that there always exists a v_s^* to make U largest with respected to different β, and the maximum of U and β changes with v_s. Under the parameters cited in this simulation, we can justice that $v_s = 0.7018$ calculated is the optimal value that maximizes SEE.

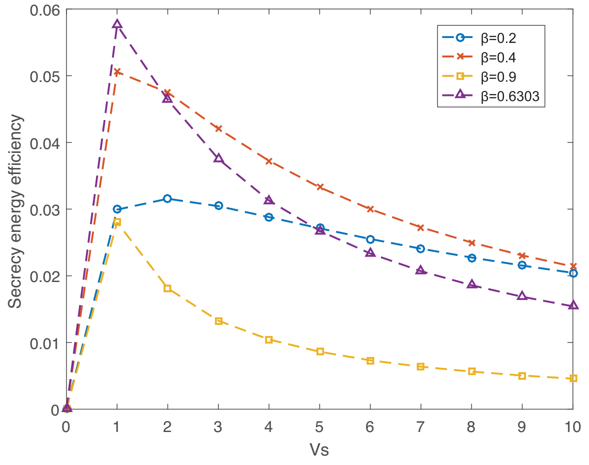

Fig. 6. The secrecy energy efficiency as a function of the energy absorption rate and energy harvesting time when energy absorption rate changes continuously.

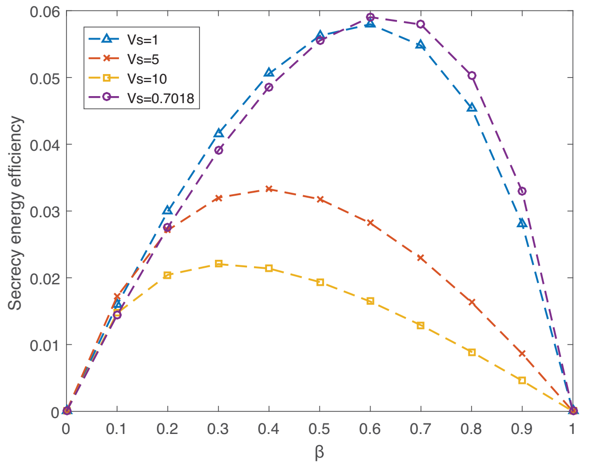

Fig. 7. The secrecy energy efficiency as a function of the energy absorption rate and energy harvesting time when changes continuously

Fig. 8 shows the comparison between the half-power ratio algorithm and the power absorption ratio in this paper. g_D denotes the channel coefficients in the information source-destination link. It is clear that the algorithm in this paper is superior to the traditional algorithm which include half-power ratio algorithm.

As can be seen from Fig. 9, with the increase of the number of energy sources, the average value of secrecy and energy efficiency becomes larger and larger, therefore, the selection of information sources can effectively improve the performance

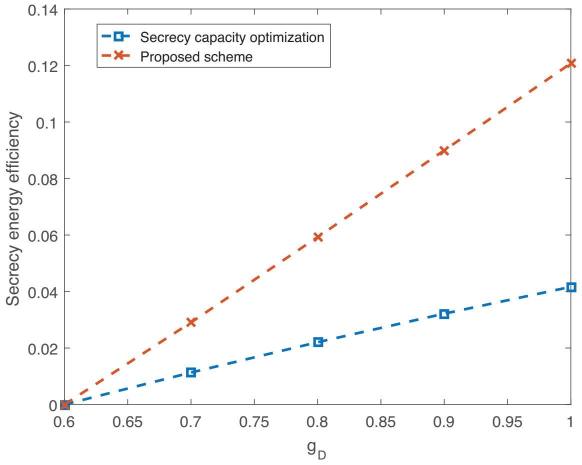

Fig. 8. The performance comparison of the optimal and half power absorption ratio algorithm

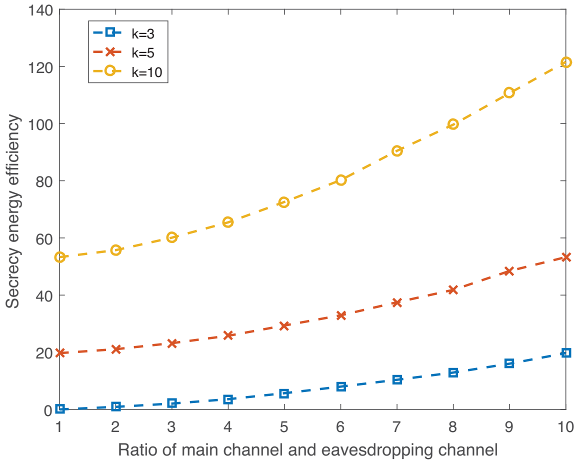

Fig. 9. Maximum secrecy energy efficiency with varying number of energy sources.

of the system.

VI. Conclusion

In this paper, we established the system model with one energy source, one information source, one destination and one eavesdrop node, based on ST protocol. To fully improve the performance of the system, we combined secrecy rate and energy efficiency and investigate the SEE of the network. Under the limited transmit power mode, we got the expression for SEE, which depends on energy absorption rate and time. Then we analyzed the system's performance based on SEE, and proposed the optimal energy source selection method. Our analytical results revealed that the secrecy energy efficiency had a maximum. Finally, we further provided simulation results based on secrecy energy efficiency maximization algorithm to demonstrate that our proposed model and methods are efficient.

Acknowledgments

This work was supported by National Natural Science Foundation of China under grants 61901241, 61671144 and 61801257, Shandong Provincial Natural Science Foundation, China under grant ZR2017BF028, Henan Province Science and Technology Research Project under grant 182102110401, Students' Plantform for Innovation and Entrepreneurship Training Program of Qingdao University, Cyrus Tang Foundation Endowed Young Scholar Program.

References

[1] H. Dai, H. Zhang, B. Wang, and L. Yang, "The multi-objective deployment optimization of UAV-mounted cache-enabled base stations," *Physical Communication*, vol. 34, pp. 114–120, June 2019.

[2] K. Song, B. Ji, and C. Li, "Resource allocation for relay-aided underwater acoustic sensor networks with energy harvesting," *Physical Communication*, vol. 33, pp. 241 – 248, 2019.

[3] K. Song, B. Ji, C. Li, and L. Yang, "Outage analysis for simultaneous wireless information and power transfer in dual-hop relaying networks," *Wireless Networks*, vol. 25, no. 2, pp. 837–844, Feb 2019.

[4] P. S. Lakshmi, M. G. Jibukumar, and V. S. Neenu, "Network lifetime enhancement of multi-hop wireless sensor network by RF energy harvesting," in *2018 International Conference on Information Networking (ICOIN)*, Jan 2018, pp. 738–743.

[5] A. Bhowmick, S. D. Roy, and S. Kundu, "Throughput of a cognitive radio network with energy-harvesting based on primary user signal," *IEEE Wireless Communications Letters*, vol. 5, no. 2, pp. 136–139, April 2016.

[6] Y. Gu and S. Aïssa, "RF-based energy harvesting in decode-and-forward relaying systems: Ergodic and outage capacities," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6425–6434, Nov 2015.

[7] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 1861–1874, May 2016.

[8] M. Hayashi, "Secure physical layer network coding versus secure network coding," in *2018 IEEE Information Theory Workshop (ITW)*, Nov 2018, pp. 1–5.

[9] H. J. Visser and R. J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: Principles and requirements," *Proceedings of the IEEE*, vol. 101, no. 6, pp. 1410–1423, June 2013.

[10] Wyner and D. A., "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] S. Gautam, T. X. Vu, S. Chatzinotas, and B. Ottersten, "Cache-aided simultaneous wireless information and power transfer (SWIPT) with relay selection," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 187–201, Jan 2019.

[12] P. S. Lakshmi, M. G. Jibukumar, and V. S. Neenu, "Network lifetime enhancement of multi-hop wireless sensor network by RF energy harvesting," in *International Conference on Information Networking*, 2018.

[13] C. Zhang and X. Jia, "Joint beamforming optimisation for noma-based wireless powered multi-pair two-way AF and DF relaying networks," *IET Communications*, vol. 13, no. 4, pp. 387–395, 2019.

[14] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[15] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3025–3038, July 2016.

[16] X. Wang, J. Liu, C. Zhai, S. Ma, and Q. Wang, "Energy efficient relay networks with wireless power transfer from a multi-antenna base station," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 4, pp. 533–543, 2016.

[17] H. Zhang and L. Duan, "Going beyond secrecy rate via information jamming," in *2018 IEEE Global Communications Conference (GLOBECOM)*, Dec 2018, pp. 1–6.