On the Placement of RF Energy Harvesting Node in Wireless Networks with Secrecy Considerations

Biao He and Xiangyun Zhou
Research School of Engineering, The Australian National University, Australia
Email: biao.he@anu.edu.au, xiangyun.zhou@anu.edu.au

***Abstract*—The potential dual use of radio-frequency (RF) signals for carrying energy and information brings an exciting opportunity for energy harvesting (EH) from ambient RF signals in wireless communication networks. To maximize the efficiency of harvesting wireless energy, it is desirable to have the EH node located close to the transmitter. However, when the transmitted information is confidential, the EH node should be regarded as a potential eavesdropper, and hence, it is preferred to have the EH node located far from the transmitter. Therefore, the placement of EH nodes in wireless networks becomes an interesting problem when secrecy is an important consideration. In this paper, we investigate the optimal placement of the EH node with physical-layer security considerations by formulating and solving two optimization problems. The first problem maximizes the average EH power subject to a secrecy outage constraint, while the second problem minimizes the secrecy outage probability subject to an EH constraint. Our results also demonstrate the tradeoff between secrecy and EH performances caused by the placement of the EH node.**

I. Introduction

Energy harvesting (EH) is a promising approach to reduce the energy consumption and prolong the lifetime of wireless networks. Apart from traditional EH sources (e.g., sunlight, air-flow and vibration), the ambient radio-frequency (RF) signal has become a new energy source that can be exploited from surrounding wireless transmissions. Different to other EH sources, RF signals can carry not only energy but also information at the same time. Thus, an increasing amount of attention has been paid to the RF energy harvesting in wireless communications, e.g., [1] and references therein.

Consider a basic wireless network where the base station transmits messages to the information receiver through RF signals. The RF signal not only reaches the information receiver, but is also broadcast into all other directions. In fact, the unused signal in those directions can be viewed as energy waste. To make the best use of RF signals and recycle such a waste of energy, EH nodes can be introduced to collect and take advantage of the energy contained in RF signals. In such a network, the information receiver obtains information from the transmitter through RF signals and the EH node takes advantage of the energy carried by ambient RF signals. Because of the mobile data traffic explosion, the issue of energy consumption will become very critical in the future wireless systems, and energy efficiency is stated as a major research theme for 5G communications [2]. Actually, for a future network with both high-power and low-power devices, the low-power devices can harvest energy from ambient RF signals to improve the energy efficiency of the entire network.

Introducing EH nodes to harvest ambient RF energy is not without drawbacks. One of the issues is that the EH nodes may become threats to the security of message transmissions in the network. When the information transmitted from the transmitter to the information receiver is (highly) confidential, EH nodes should be treated as potential eavesdroppers in the network. The security issue in wireless networks with EH nodes was studied very recently, e.g., [3, 4]. Liu et al. [3] addressed the physical layer security problem in the wireless networks with EH nodes and assumed that the transmitter has perfect channel state information (CSI) of both the EH node and the information receiver. Ng et al. [4] investigated a similar problem, while considering the scenarios where transmitter has only partial or no CSI of the EH node. It is worth noting that both [3] and [4] investigated the secrecy issue of transmissions from the physical-layer security perspective. After the pioneering work of [5] by Wyner and [6] by Csiszár and Körner, physical layer security has been widely investigated during the past decades [7, 8]. Regarded as a complement to the cryptographic technology, physical layer security increases the security of wireless transmissions by exploring fading properties of the channel but does not rely on the encryption.

It is pointed out in [3] that having the EH node closer to the transmitter than the information receiver incurs a challenge to the transmission security, because the potential eavesdropper has better channel than the information receiver. Hence, if the location of the EH node is controllable in the system, the EH node should be placed far from the transmitter to increase the security of communications. On the other hand, to collect the energy from transmitter efficiently, it is wise to have the EH node close to the transmitter. This naturally arises an interesting problem on the placement of the EH node in secrecy wireless networks.

Motivated by this problem, we investigate the effect of different placements of the EH node in wireless systems with physical-layer security considerations. Two optimization problems of the EH node's placement for different practical aims are addressed. The first problem maximizes the average EH power at the EH node subject to a secrecy outage constraint, while the second problem minimizes the secrecy outage probability subject to an EH constraint. The optimal solutions of the EH node's placement to both problems are obtained. In addition, the analytical and numerical results present the tradeoff between secrecy and EH performances in a system caused by the placement of the EH node.

It is worth mentioning that most of current researches related

to the RF energy harvesting in wireless communications (including this work) are largely theoretically oriented. In practice, the placement of EH node is not always controllable by the system designer, for example, when the EH node is a user in the network. However, in this work, we do not consider the EH node as a user to be served in the wireless system. The purpose of introducing the EH node is to recycle the energy waste and increase the energy efficiency. Besides, the node placement has been an important problem of study in different networks, e.g., wireless sensor networks, relay networks, and cellular networks. However, no previous work has specifically studied the placement of EH nodes in secrecy networks.

The remainder of this paper is organized as follows. Section II introduces the system model and performance measures. Section III addresses the optimization problems and provides analytical solutions. Numerical results and conclusions are given in Sections IV and V, respectively.

II. System Model

We consider a wireless system where a transmitter, Alice, wants to send confidential information to a receiver, Bob. In addition, an EH node, Eve, is introduced to collect and take advantage of energy from the information-carrying RF signals.[1] To secure the information transmitted from Alice to Bob, Eve is regarded as a potential eavesdropper in the system [3]. Although a single EH node is considered in this work, the analysis can be easily extended to multiple EH nodes (regarded as non-colluding eavesdroppers).

The received signal at Bob or Eve can be written as

$$y_i = \frac{\sqrt{P}h_i x}{1+\sqrt{d_i^m}} + n_i, \quad i = b \text{ or } e, \tag{1}$$

where the subscripts b and e denote the parameters for Bob and Eve, respectively. In addition, P denotes the transmit power, m denotes the path-loss exponent, d_i denotes the distance from Alice to Bob or Eve, $h_i \sim \mathcal{CN}(0,1)$ denotes the Rayleigh fading channel gain, $n_i \sim \mathcal{CN}(0,1)$ denotes the additive white noise, x denotes the normalized transmitted signal, i.e., $E\left\{|x|^2\right\} = 1$, where $\mathcal{CN}(0,1)$ represents the zero mean complex Gaussian distribution with unit variance and $E\{\cdot\}$ is the expectation operation. The bounded path-loss model is adopted in (1) to avoid the singularity at $d_i \to 0$ [9].

The instantaneous received signal power can be written as

$$P_i = \frac{P|h_i|^2}{\left(1+\sqrt{d_i^m}\right)^2}, \quad i = b \text{ or } e, \tag{2}$$

having an exponential distribution given by

$$f_{P_i}(P_i) = \frac{1}{\bar{P}_i}\exp\left(-\frac{P_i}{\bar{P}_i}\right), \tag{3}$$

where $\bar{P}_i = E\left\{P_i\right\} = \frac{P}{\left(1+\sqrt{d_i^m}\right)^2}$ is the average received signal power over different fading states. Please note that the value of received signal power is equal to the received signal to noise ratio (SNR), since unit-variance noise, n_i, is assumed.

[1]The intended use of the collected energy at Eve is beyond the scope of this work.

Bob and Eve are assumed to perfectly know their own channels. Alice perfectly knows Bob's instantaneous CSI, but only has the statistical knowledge on Eve's channel. Eve's instantaneous CSI is assumed unknown at Alice, because Eve is not a user served by the transmitter.

A. On-Off Transmission Scheme

To improve the secrecy performance of transmissions, the on-off scheme [10, 11] for message transmissions is considered. In general, Alice decides whether or not to transmit according to the instantaneous CSI on Bob's channel. For example, if Alice knows that Bob's channel is bad, she would naturally suspend the transmission.

Specifically, the transmission takes place whenever the instantaneous received signal power at Bob, P_b, exceeds some power threshold μ. Thus, there exists a probability of transmission, which is given by

$$p_{\text{tx}} = \Pr(P_b > \mu) = \exp\left(-\frac{\mu}{\bar{P}_b}\right), \tag{4}$$

where $\Pr(\cdot)$ denotes the probability measure. When the transmission is suspended, Alice does not intentionally transmit RF signals carrying only energy to charge Eve. This is because that Eve is introduced to collect and take advantage of energy from the information-carrying RF signals, and it is not a user served by Alice.

Having the on-off transmission scheme to secure the transmission, indeed, incurs some delay on the message transmission. Since this paper focuses on the tradeoff between secrecy and EH performances, the delay issue is not specifically investigated. In addition, if the delay issue is very critical to the transmission, the analysis can be easily extended by adding a delay constraint, i.e., $p_{tx} \geq \tau$.

B. EH Performance Measure

The EH performance of the system is measured by the average EH power at Eve over time and different fading states [12]. Since the transmission does not always happen due to the on-off scheme, the average EH power over time for a given fading state of Eve's channel can be expressed as

$$Q = \alpha p_{\text{tx}} P_e = \alpha \exp\left(-\frac{\mu}{\bar{P}_b}\right) P_e, \tag{5}$$

where $0 < \alpha \leq 1$ is a constant that accounts for the loss of energy transducer for converting the harvested energy to electrical energy to be stored. Then, averaging (5) over different fading states of Eve's channel, the overall average EH power is given by

$$\bar{Q} = E\{Q\} = \alpha \exp\left(-\frac{\mu}{\bar{P}_b}\right) \bar{P}_e. \tag{6}$$

C. Secrecy Performance Measure

The secrecy performance of the system is measured by the secrecy outage probability [13]. The secrecy outage probability is given by

$$p_{\text{so}} = \Pr\left(C_b - C_e < R_s \mid \text{message transmission}\right), \tag{7}$$

where R_s is a target secrecy rate, $C_b = \log_2(1+P_b)$ and $C_e = \log_2(1+P_e)$ are Bob and Eve's channel capacities. The probability is conditioned on message transmission due to the on-off scheme.

In this paper, we focus on the special case of $R_s \to 0$, which has been widely considered in literatures, e.g., [14, 15]. This case is relevant in scenarios where throughput is not an important concern but secrecy is crucial. Hence, the confidential information is transmitted at a very low rate and the secrecy performance is measured by the probability that a perfectly secure link exists between Alice and Bob at an arbitrarily small rate:

$$\begin{aligned} p_{\text{so}} &= \Pr\left(C_b < C_e \mid \text{message transmission}\right) \\ &= \Pr\left(P_b < P_e \mid P_b > \mu\right) \\ &= \frac{\Pr\left(\mu < P_b < P_e\right)}{\Pr\left(P_b > \mu\right)} \\ &= \exp\left(\frac{\mu}{\bar{P}_b}\right) \int_{\mu}^{\infty} \left(\int_{\mu}^{P_e} f_{P_b}(P_b) \mathrm{d}P_b \right) f_{P_e}(P_e) \mathrm{d}P_e \\ &= \frac{\bar{P}_e}{\bar{P}_e + \bar{P}_b} \exp\left(-\frac{\mu}{\bar{P}_e}\right). \end{aligned} \tag{8}$$

It is worth mentioning that the analysis can be easily extended to the case of having a fixed transmission rate $R_s > 0$, for taking the throughput performance into account. In this work, we only focus on the tradeoff between secrecy and EH performances in the system caused by the placement of the EH node, and leave the analysis on throughput performance for future work.

III. Problem Formulation and Solution

As discussed earlier, the placement of the EH node arises an interesting tradeoff between secrecy and EH performances of the system. Without the secrecy consideration, the EH node should be placed close to the transmitter. On the contrary, without the EH concern, it is desirable to have the potential eavesdropper far from the transmitter. Thus, the optimal placement of the EH node becomes an interesting problem, when both secrecy and EH performances are considered in the system.

The placement of the EH node is reflected by the distance from Alice to Eve, d_e. In this work, we investigate how the value of d_e affects both secrecy and EH performances of the system. Specifically, two optimization problems for different practical aims are analyzed in this section. The first problem maximizes the average EH power subject to a secrecy outage constraint, while the second problem minimizes the secrecy outage probability subject to an EH constraint. In each problem, we solve for the optimal placement of the EH node.

The ratio of $\bar{P}_e$ to $\bar{P}_b$ is introduced for convenience, which is given by

$$\rho = \frac{\bar{P}_e}{\bar{P}_b} = \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_e^m}\right)^2}. \tag{9}$$

Instead of solving the optimal d_e directly, we find the optimal ρ for each problem, and then the optimal d_e can be easily derived by

$$d_e = \left(\frac{1 + d_b^{\frac{m}{2}}}{\rho^{\frac{1}{2}}} - 1 \right)^{\frac{2}{m}}. \tag{10}$$

Moreover, since the on-off transmission scheme is adopted, the on-off power threshold, μ, is another parameter to optimize. Therefore, the parameters to optimize are ρ and μ in the following problems. The feasible domain of ρ is $0 < \rho \leq \left(1+\sqrt{d_b^m}\right)^2$ corresponding to the feasible domain of d_e from 0 to ∞. The feasible domain of μ is $0 \leq \mu < \infty$.

A. Maximizing Average EH Power with Secrecy Constraint

For a given secrecy constraint $p_{\text{so}} \leq \epsilon$, our objective is to find the optimal ρ and μ that maximize $\bar{Q}$. Here $0 < \epsilon \leq 1$ denotes the maximal acceptable secrecy outage probability in the system. The optimization problem can be formulated as

$$\max_{\mu,\rho} \quad \bar{Q}(\mu,\rho) = \alpha \exp\left(-\frac{\mu}{\bar{P}_b}\right) \rho \bar{P}_b, \tag{11}$$

$$\text{s.t.} \quad p_{\text{so}} \leq \epsilon, \mu \geq 0, 0 < \rho \leq \left(1+\sqrt{d_b^m}\right)^2. \tag{12}$$

The solution to the problem above is given by the following proposition.[2]

Proposition 1: The optimal parameters for maximizing the average EH power subject to the secrecy outage constraint are given as follows:

$$\mu = \begin{cases} \frac{\rho P}{\left(1+\sqrt{d_b^m}\right)^2} \ln\left(\frac{\rho}{\epsilon(\rho+1)}\right) & \text{if } \epsilon < \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}, \\ 0 & \text{otherwise,} \end{cases} \tag{13}$$

$$\rho = \begin{cases} k_1 & \text{if } \epsilon < \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1} \exp\left(-\frac{1}{\left(1+\sqrt{d_b^m}\right)^2+\left(1+\sqrt{d_b^m}\right)^4}\right), \\ \left(1+\sqrt{d_b^m}\right)^2 & \text{otherwise,} \end{cases} \tag{14}$$

where k_1 is the solution of ρ to the equation

$$\frac{1}{\rho+1} + \rho \ln\left(\frac{\epsilon(\rho+1)}{\rho}\right) = 0. \tag{15}$$

Proof: From (11), we see that $\bar{Q}$ is a decreasing function of μ for any given ρ. Thus, we can solve the optimization problem by the following three steps: 1. Deriving the expression of minimal μ for any given ρ, $\mu_{\min}(\rho)$. 2. Substituting $\mu_{\min}(\rho)$ into (11) to get the expression of $\bar{Q}$ as a function of ρ, $\bar{Q}(\rho)$. 3. Solving the optimal ρ that maximizes the overall $\bar{Q}$.

Step 1: From $\rho \leq \left(1+\sqrt{d_b^m}\right)^2$ and (8), we see that p_{so} is always less than $\frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}$. Hence when $\epsilon \geq \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}$, the minimal μ does not depends on ρ, and $\mu_{\min}(\rho) = 0$. When $\epsilon < \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}$, the minimal μ is related to ρ, which is given by

$$\mu_{\min}(\rho) = \begin{cases} \bar{P}_b \rho \ln\left(\frac{\rho}{\epsilon(\rho+1)}\right) & \text{if } \rho > \frac{\epsilon}{1-\epsilon}, \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

[2]Although there is no closed-form solution of k_1 in Proposition 1, it can be easily solved explicitly for any value of ϵ by mathematical software, e.g. MATLAB.

Steps 2 and 3: When $\epsilon \geq \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}$, substituting $\mu_{\min}(\rho)=0$ into (11), the optimization problem changes to

$$\max_{\rho} \quad \bar{Q}(\rho)=\alpha\rho\bar{P}_b, \tag{17}$$

$$\text{s.t.} \quad 0<\rho\leq\left(1+\sqrt{d_b^m}\right)^2. \tag{18}$$

The maximal $\bar{Q}$ is then achieved at

$$\rho=\left(1+\sqrt{d_b^m}\right)^2. \tag{19}$$

When $\epsilon < \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}$, substituting (16) into (11), we have

$$\begin{aligned}\bar{Q}(\rho) &= \begin{cases} \exp\left(\rho\ln\left(\frac{\epsilon(\rho+1)}{\rho}\right)\right)\alpha\rho\bar{P}_b & \text{if} \quad \rho>\frac{\epsilon}{1-\epsilon}, \\ \alpha\rho\bar{P}_b & \text{otherwise,}\end{cases} \\ &= \begin{cases} \left(\frac{\epsilon(\rho+1)}{\rho}\right)^{\rho}\alpha\rho\bar{P}_b & \text{if} \quad \rho>\frac{\epsilon}{1-\epsilon}, \\ \alpha\rho\bar{P}_b & \text{otherwise,}\end{cases}\end{aligned} \tag{20}$$

and then the optimization problem changes to

$$\max_{\rho} \quad \bar{Q}(\rho)=\begin{cases} \left(\frac{\epsilon(\rho+1)}{\rho}\right)^{\rho}\alpha\rho\bar{P}_b & \text{if} \quad \rho>\frac{\epsilon}{1-\epsilon}, \\ \alpha\rho\bar{P}_b & \text{otherwise,}\end{cases} \tag{21}$$

$$\text{s.t.} \quad 0<\rho\leq\left(1+\sqrt{d_b^m}\right)^2. \tag{22}$$

For $0<\rho\leq\frac{\epsilon}{1-\epsilon}$, the maximal $\bar{Q}$ is achieved at $\rho=\frac{\epsilon}{1-\epsilon}$. For $\rho>\frac{\epsilon}{1-\epsilon}$, we can find that an extremum of $\bar{Q}$ would be achieved at k_1 which is the solution of ρ to the equation

$$\frac{\partial\bar{Q}}{\partial\rho}=0\Leftrightarrow\frac{1}{\rho+1}+\rho\ln\left(\frac{\epsilon(\rho+1)}{\rho}\right)=0. \tag{23}$$

It can be found that $\frac{\partial^2\bar{Q}}{\partial^2\rho}<0$ for $\rho>\frac{\epsilon}{1-\epsilon}$. Thus, $\bar{Q}(k_1)$ is a maximum of $\bar{Q}$ for $\rho>\frac{\epsilon}{1-\epsilon}$, and $\bar{Q}$ increases as ρ increases from $\frac{\epsilon}{1-\epsilon}$ to k_1. Because the feasible ρ is upper bounded by $\left(1+\sqrt{d_b^m}\right)^2$, the optimal ρ in the range of $\frac{\epsilon}{1-\epsilon}<\rho<\left(1+\sqrt{d_b^m}\right)^2$ is given by

$$\rho=\min\left\{k_1,\left(1+\sqrt{d_b^m}\right)^2\right\}. \tag{24}$$

Moreover, from (23), we see that k_1 is an increasing function of ϵ, and $\epsilon=\frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}\exp\left(-\frac{1}{\left(1+\sqrt{d_b^m}\right)^2+\left(1+\sqrt{d_b^m}\right)^4}\right)$ when $k_1=\left(1+\sqrt{d_b^m}\right)^2$. Hence, (24) can be rewritten as (14). Besides, we see that k_1 is always larger than $\rho=\frac{\epsilon}{1-\epsilon}$. This indicates that the maximum $\bar{Q}$ achieved in the range of $\rho>\frac{\epsilon}{1-\epsilon}$ is always larger than the maximum $\bar{Q}$ achieved in the range of $\rho\leq\frac{\epsilon}{1-\epsilon}$. Hence, (14) actually is the optimal ρ over $0<\rho\leq\left(1+\sqrt{d_b^m}\right)^2$ when $\epsilon<\frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1}$, and the corresponding $\mu_{\min}(\rho)=\bar{P}_b\rho\ln\left(\frac{\rho}{\epsilon(\rho+1)}\right)$.

Finally, the optimal solutions of μ and ρ are given as (13) and (14) in Proposition 1. ■

B. Minimizing Secrecy Outage Probability with EH Constraint

For a given average EH power constraint $\bar{Q}\geq\delta$, our objective is to find the optimal ρ and μ that minimize p_{so}. Here $0\leq\delta\leq\alpha P$ denotes the minimal acceptable average EH power to maintain the EH node's own operation. The optimization problem can be formulated as

$$\min_{\mu,\rho} \quad p_{\text{so}}(\mu,\rho)=\frac{\rho}{\rho+1}\exp\left(-\frac{\mu}{\rho\bar{P}_b}\right), \tag{25}$$

$$\text{s.t.} \quad \bar{Q}\geq\delta,\mu\geq0,0<\rho\leq\left(1+\sqrt{d_b^m}\right)^2. \tag{26}$$

The solution to the problem above is given by the following proposition.[3]

Proposition 2: The optimal parameters for minimizing the secrecy outage probability subject to the EH constraint are given as follows:

$$\mu=\frac{P}{\left(1+\sqrt{d_b^m}\right)^2}\ln\left(\frac{\alpha\rho P}{\delta\left(1+\sqrt{d_b^m}\right)^2}\right), \tag{27}$$

$$\rho=\begin{cases} k_2 & \textit{if} \quad \delta<\exp\left(-\frac{1}{1+\left(1+\sqrt{d_b^m}\right)^2}\right)\alpha P, \\ \left(1+\sqrt{d_b^m}\right)^2 & \textit{otherwise,}\end{cases} \tag{28}$$

where k_2 is the solution of ρ to the equation

$$1+(1+\rho)\ln\frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha\rho P}=0. \tag{29}$$

Proof: From (25), we see that p_{so} is a decreasing function of μ for any given ρ. Thus, we can solve the optimization problem by the following three steps: 1. Deriving the expression of maximal μ for any given ρ, $\mu_{\max}(\rho)$. 2. Substituting $\mu_{\max}(\rho)$ into (25) to get the expression of p_{so} as a function of ρ, $p_{\text{so}}(\rho)$. 3. Solving the optimal ρ that minimizes the overall p_{so}.

Step 1: From $\bar{Q}\geq\delta$, we have

$$\mu_{\max}(\rho)=\bar{P}_b\ln\left(\frac{\alpha\rho\bar{P}_b}{\delta}\right). \tag{30}$$

Since $\mu\geq0$ and (30), we have

$$\rho\geq\frac{\delta}{\alpha\bar{P}_b}=\frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha P}. \tag{31}$$

Step 2: Substituting (30) into (25), we have

$$p_{\text{so}}(\rho)=\frac{\rho}{\rho+1}\exp\left(-\frac{\ln\frac{\alpha\rho\bar{P}_b}{\delta}}{\rho}\right)=\frac{\rho}{\rho+1}\left(\frac{\delta}{\alpha\rho\bar{P}_b}\right)^{\frac{1}{\rho}}. \tag{32}$$

Then, the optimization problem changes to

$$\min_{\rho} \quad p_{\text{so}}(\rho)=\frac{\rho}{\rho+1}\left(\frac{\delta}{\alpha\rho\bar{P}_b}\right)^{\frac{1}{\rho}}, \tag{33}$$

$$\text{s.t.} \quad \frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha P}\leq\rho\leq\left(1+\sqrt{d_b^m}\right)^2. \tag{34}$$

[3]Although there is no closed-form solution of k_2 in Proposition 2, it can be easily solved explicitly for any value of δ by mathematical software, e.g. MATLAB.

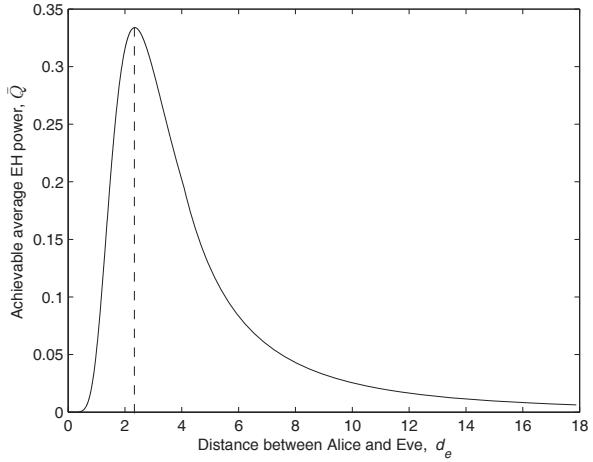

Fig. 1. Achievable average EH power versus the distance between Alice and Eve for a given secrecy outage probability constraint. The system parameters are $\epsilon = 0.2, d_b = 2, \alpha = 0.9, m = 2.5, P = 10$ dB.

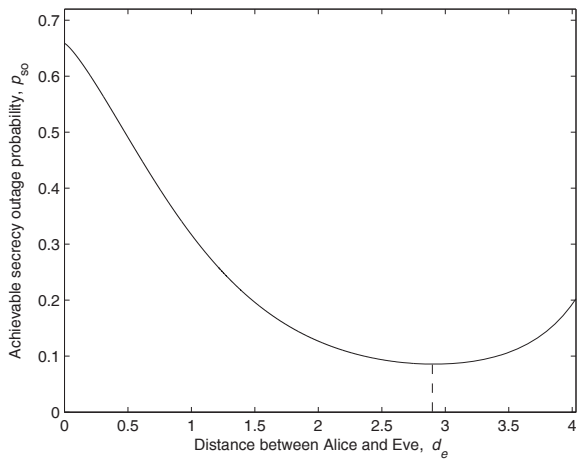

Fig. 2. Achievable secrecy outage probability versus the distance between Alice and Eve for a given average EH power constraint. The system parameters are $\delta = 0.2, d_b = 2, \alpha = 0.9, m = 2.5, P = 10$ dB.

Step 3: We can find that an extremum of p_{so} would be achieved at k_2 which is the solution of ρ to the equation

$$\frac{\partial p_{\text{so}}}{\partial \rho} = 0 \Leftrightarrow -\left(1 + (1+\rho)\ln\frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha\rho P}\right) = 0. \quad (35)$$

It can be found that k_2 is always larger than $\frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha P}$ and $\frac{\partial^2 p_{\text{so}}}{\partial^2 \rho} > 0$ for $\rho > \frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha P}$. Thus, $p_{\text{so}}(k_2)$ is a minimum of p_{so} for $\rho \geq \frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha P}$, and p_{so} decreases as ρ increases from $\frac{\delta\left(1+\sqrt{d_b^m}\right)^2}{\alpha P}$ to k_2. Because the feasible ρ is upper bounded by $\left(1+\sqrt{d_b^m}\right)^2$, the optimal ρ is given by

$$\rho = \min\left\{k_2, \left(1+\sqrt{d_b^m}\right)^2\right\}. \quad (36)$$

Moreover, from (35), we see that k_2 is an increasing function of δ, and $\delta = \exp\left(-\frac{1}{1+\left(1+\sqrt{d_b^m}\right)^2}\right)\alpha P$ when $k_2 = \left(1+\sqrt{d_b^m}\right)^2$. Hence, (36) can be rewritten as (28).

Finally, the optimal solutions of μ and ρ are given as (27) and (28) in Proposition 2. ■

IV. Numerical Results

In this section, the numerical results are presented to demonstrate the effect of EH node placement on systems with both secrecy and EH considerations.

Figure 1 illustrates the achievable average EH power for different placements of the EH node subject to a given secrecy outage constraint. Figure 2 presents the achievable secrecy outage probability for different placements of the EH node subject to a given EH constraint. From both figures, we see that the placement of the EH node, i.e., the distance between Alice and Eve, noticeably influences the system performance. A good choice of the distance between the transmitter and the EH node can indeed optimize the system performance, i.e., maximizing the average EH power in Figure 1 or minimizing the secrecy outage probability in Figure 2. Therefore, it is necessary to investigate the optimal placement of the EH node for systems with both secrecy and EH considerations.

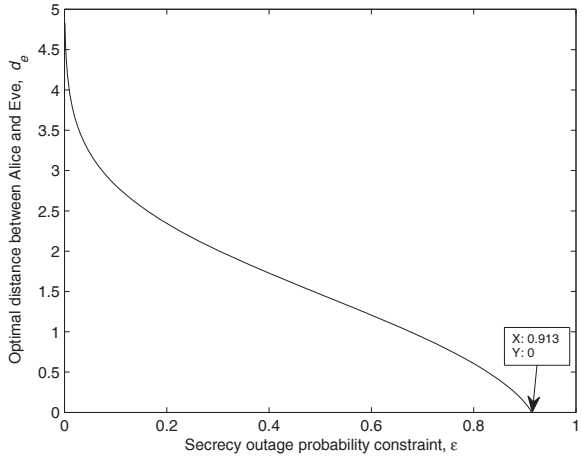

Fig. 3. To maximize the average EH power: optimal distance between Alice and Eve versus secrecy outage constraint. The system parameters are $d_b = 2, \alpha = 0.9, m = 2.5, P = 10$ dB.

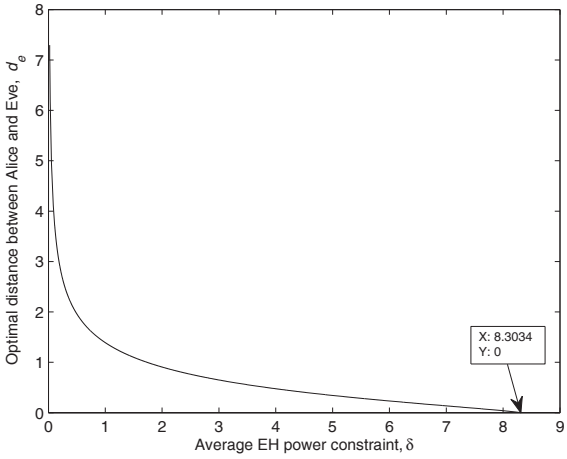

Fig. 4. To minimize the secrecy outage probability: optimal distance between Alice and Eve versus EH constraint. The system parameters are $d_b = 2, \alpha = 0.9, m = 2.5, P = 10$ dB.

Figure 3 presents the optimal distances between the transmitter and the EH node that maximize the average EH power subject to different secrecy outage constraints. Figure 4 demonstrates the optimal distances between the transmitter and the EH node that minimize the secrecy outage probability subject to different EH constraints. As shown in Figure 3, the optimal distance decreases as the secrecy outage constraint becomes loose. In contrast, the optimal distance in Figure 4 decreases as the EH constraint becomes stringent. In addition, we find that it is optimal to place the EH node as close as possible to the transmitter once the secrecy constraint is looser than a certain level, i.e.,

$$\epsilon \geq \frac{\left(1+\sqrt{d_b^m}\right)^2}{\left(1+\sqrt{d_b^m}\right)^2+1} \exp\left(-\frac{1}{\left(1+\sqrt{d_b^m}\right)^2+\left(1+\sqrt{d_b^m}\right)^4}\right)=0.913$$

derived from from (14), or the EH constraint is more stringent than a certain level, i.e.,

$$\delta \geq \exp\left(-\frac{1}{1+\left(1+\sqrt{d_b^m}\right)^2}\right) \alpha P = 8.3034$$

derived from (28). This observation indicates that, in some scenarios, it can still be optimal to place the EH node as close to the transmitter as possible even when both secrecy and EH performances are considered.

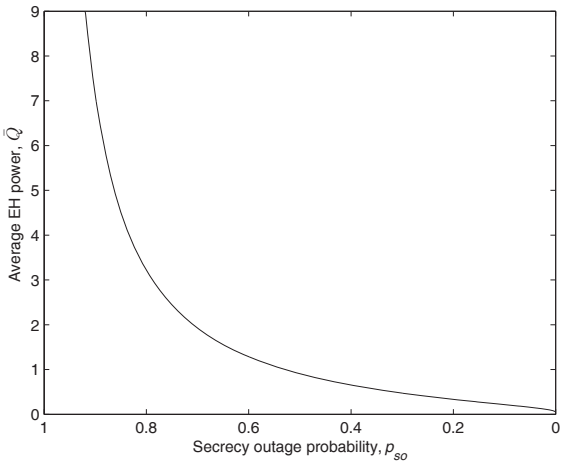

Fig. 5. Average EH power versus secrecy outage probability. The system parameters are $d_b = 2, \alpha = 0.9, m = 2.5, P = 10$ dB.

Figure 5 demonstrates the tradeoff between secrecy and EH performances caused by the placement of the EH node. Note that the x-axis of the figure ranges from the highest secrecy outage probability, $p_{\text{so}} = 1$, to the smallest secrecy outage probability, $p_{\text{so}} = 0$. The area below the curve represents the achievable secrecy-EH region which consists of all achievable pairs of the secrecy outage probability and the average EH power. The (p_{so}, $\bar{Q}$) pairs on the curve (i.e., the boundary of the secrecy-EH region) can be obtained by either the optimal EH node placement given in Proposition 1 with different secrecy constraints on p_{so} or the optimal EH node placement given in Proposition 2 with different EH constraints on $\bar{Q}$. As shown by the curve, to achieve better EH performance, the secrecy performance of the system has to be scarified, and vice versa.

V. Conclusions

In this paper, we addressed the issue of EH node placement in wireless networks with both secrecy and EH considerations. The optimal distance between the transmitter and the EH node is investigated to maximize the average EH power subject to the constraint on secrecy outage probability, or vise verse. In addition, the numerical results present the achievable secrecy-EH region, which illustrates the tradeoff between secrecy and EH performances of wireless networks.

Acknowledgement

The authors wish to thank Dr. Chin Keong Ho for helpful suggestions and fruitful discussions.

References

[1] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," 2014. [Online]. Available: http://arxiv.org/abs/1406.6470

[2] J. G. Andrews, S. Buzzi, W. Choi, S. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, 2014, to appear.

[3] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, Jan. 2014.

[4] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, 2014, to appear.

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

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[8] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[9] H. Inaltekin, M. Chiang, H. V. Poor, and S. B. Wicker, "On unbounded path-loss models: effects of singularity on wireless network performance," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1078–1092, Sept. 2009.

[10] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[11] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[12] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288–300, Jan. 2013.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[14] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[15] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.