Secrecy Outage Probability of Wirelessly Powered Wiretap Channels

Xin Jiang*, Caijun Zhong*, Xiaoming Chen† and Zhaoyang Zhang*
* Zhejiang Provincial Key Laboratory of Information Processing, Communication and Networking, Zhejiang University, China
† College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China
Email: {xinjiang, caijunzhong, ning_ming }@zju.edu.cn, chenxiaoming@nuaa.edu.cn

***Abstract*—This paper considers a wirelessly powered wiretap channel, where an energy constrained information source, powered by a dedicated power beacon, communicates with a legitimate user in the presence of a passive eavesdropper. The source is assumed to have multiple antennas, while the other three nodes are equipped with a single antenna each. Considering a simple time-switching design where power transfer and information transmission are separated in time. We investigate two popular transmission schemes, namely maximum ratio transmission (MRT) and transmit antenna selection (TAS). Closed-form expressions are derived for the achievable secrecy outage probability of both schemes. In addition, simple approximations are obtained at the high signal-to-noise ratio (SNR) regime. Our results demonstrate that the more channel state information (CSI) available, the better the secrecy performance. For instance, with full CSI of the main channel, the system can achieve substantial secrecy diversity gain. On the other hand, without the CSI of the main channel, no diversity gain can be attained. Finally, our theoretical claims are validated by the numerical results.**

I. Introduction

With the pressing issue of providing secure wireless communications, physical layer security, as an alternative to conventional cryptographic approaches, has gained enormous interests in recent years. The basic concept behind physical layer security is to exploit the physical layer characteristics of wireless channels to provide perfect secrecy. Since the pioneering work by Wyner in [1], which confirmed that perfect secrecy can be achieved when the quality of the wiretap channel is a degraded version of the main channel, a plethora of works have investigated various aspects of physical layer security [2–5].

On the other hand, the rapidly increasing demands for high data rate wireless services have put a tremendous pressure on the energy consumption of battery-powered mobile devices. Hence, how to prolong the lifetime of these energy-constrained mobile devices has become a critical problem to be addressed. Responding to this, a novel network architecture capitalizing on the technique of microwave power transfer was proposed in [6], where a dedicated station called power beacon is incorporated into the wireless network to power mobile devices. The performance of wirelessly powered systems was later studied for different system models including point-to-point systems [7] and dual-hop relaying systems [8].

In this paper, we propose a new wirelessly powered wiretap channel consisting of a dedicated power beacon, an energy constrained information source and a legitimate user in the presence of a passive eavesdropper. We consider the case that the source communicates with the legitimate user using the energy harvested via wireless power transfer from the power beacon. To leverage the multiple antennas at the source, two popular transmission schemes, namely maximum ratio transmission (MRT) and transmit antenna selection (TAS) are applied, and the corresponding secrecy outage performance is investigated in detail.

Our main contribution is the derivation of closed-form expressions for the achievable secrecy outage probability of the proposed schemes, which enable efficient evaluation of the achievable secrecy performance. In addition, some simple high signal-to-noise ratio (SNR) approximations are presented. Analytical results demonstrate that with global channel state information (CSI) of the main channel, the system attains full secrecy diversity gain, while only unit secrecy diversity order can be achieved with only the CSI of the wiretap channel.

Notation: We use bold lower case letters to denote vectors and lower case letters to denote scalars. $\|\mathbf{h}\|$ denotes the Frobenius norm; $\mathrm{E}\{x\}$ stands for the expectation of the random variable x; T denotes the transpose operator and $'$ denotes the conjugate operator. $\mathbf{I}_k$ is the identity matrix of size k. $\Gamma(x)$ is the gamma function [9, Eq. (8.31)] and $K_v(x)$ is the v-th order modified Bessel function of the second kind [9, Eq. (8.407.1)].

II. System Model

We consider a four-node wirelessly powered wiretap channels consisting of one power beacon PB, one source Alice and one legitimate user Bob in the presence of one eavesdropper Eve as shown in Fig. 1. We assume that the source is equipped with N antennas, while the other three nodes are equipped with a single antenna each. Quasi-static fading is assumed, such that the channel coefficients remain unchanged during each transmission block but vary independently between different blocks.

We adopt the time-sharing protocol proposed in [10]. Hence, a complete transmission slot with time duration of T is divided into two orthogonal sub-slots, i.e., one for power transfer with time duration of θT and the other for information transmission with time duration of $(1-\theta)T$.

During the first phase, the PB sends an energy signal to Alice, and the received energy signal at Alice $\mathbf{y}_s$ can be expressed as

$$\mathbf{y}_s = \sqrt{P_S}\mathbf{h}_P x_s + \mathbf{n}_s, \tag{1}$$

This work is supported by the Zhejiang Provincial Natural Science Foundation of China (No. LR15F010001), and the Fundamental Research Funds for the Central Universities (2016QNA5004). The work of X. Chen is supported by the National Natural Science Foundation of China (No. 61301102).

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

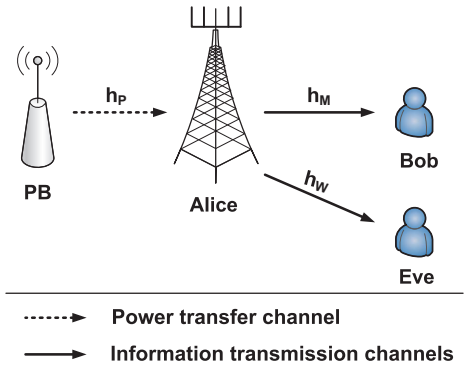

Fig. 1. A schematic diagram of the system model consisting of a power beacon PB, a source Alice, a legitimate user Bob and an eavesdropper Eve.

where P_S denotes the transmit power of the PB, x_s is the energy signal with unit power, $\mathbf{n}_s$ is an N-dimensional additive white Gaussian noise (AWGN) vector with $\mathrm{E}\{\mathbf{n}_s\mathbf{n}_s^\dagger\} = N_0\mathbf{I}$. The $N \times 1$ vector $\mathbf{h}_P$ denotes the power transfer channel from PB to Alice. Due to relatively short distance between the power beacon and the source, it is likely that the line-of-sight propagation exists. Hence, the Nakagami-m distribution is used to model the power transfer channel, i.e., the amplitude of each element of $\mathbf{h}_P$ follows Nakagami-m distribution with shape parameter m and average power λ_P.[1]

Therefore, at the end of the first phase, the total harvested energy within the duration θT can be expressed as

$$E = \eta P_S ||\mathbf{h}_P||^2 \theta T, \tag{2}$$

where η $(0 < \eta < 1)$ denotes the energy conversion efficiency.

Since the source communicates with the legitimate user during the second phase with duration $(1-\theta)T$, the transmit power can be computed as

$$P = \frac{E}{(1-\theta)T} = \eta P_S ||\mathbf{h}_P||^2 \frac{\theta}{1-\theta}. \tag{3}$$

To exploit the multiple antennas at Alice, different transmission schemes can be adopted. In this work, we consider two popular transmission schemes, namely maximum ratio transmission and transmit antenna selection.

A. Maximum Ratio Transmission (MRT)

For the MRT scheme, Alice aims at maximizing the reception quality of the main channel, as such, the received signal y_M at Bob can be written as

$$y_M = \sqrt{P}\mathbf{h}_M^T \mathbf{w} x_t + n_M, \tag{4}$$

where x_t denotes the information symbol with unit energy, the $N \times 1$ vector $\mathbf{h}_M$ denotes the main channel from Alice to Bob, whose elements are circularly symmetric complex Gaussian random variables with mean zero and variance λ_M and n_M denotes the AWGN with zero mean and variance N_0. $\mathbf{w}$ is the MRT vector given by $\mathbf{w} = \frac{\mathbf{h}_M^{'}}{||\mathbf{h}_M||}$.

[1]In the presence of line-of-sight effect, Rician fading is commonly used in literature. However, the analysis with Rician fading is much more involved. As such, for mathematical tractability, we adopt the Nakagami-m fading model, since the Nakagami-m distribution provides very accurate approximation to the Rician distribution.

Similarly, the signal received at Eve y_W can be expressed as

$$y_W = \sqrt{P}\mathbf{h}_W^T \mathbf{w} x_t + n_W, \tag{5}$$

where the $N \times 1$ vector $\mathbf{h}_W$ denotes the wiretap channel from Alice to Eve, whose elements are circularly symmetric complex Gaussian random variables with zero mean and variance λ_W, and n_W denotes the AWGN with zero mean and variance N_0.

As such, the instantaneous SNR at Bob γ_M and at Eve γ_W are given by

$$\gamma_M = \frac{\eta P_S ||\mathbf{h}_P||^2 ||\mathbf{h}_M||^2}{N_0} \frac{\theta}{1-\theta}, \tag{6}$$

and

$$\gamma_W = \frac{\eta P_S ||\mathbf{h}_P||^2 \frac{|\mathbf{h}_W^T \mathbf{h}_M^{'}|^2}{||\mathbf{h}_M||^2}}{N_0} \frac{\theta}{1-\theta}, \tag{7}$$

respectively.

B. Transmit Antenna Selection (TAS)

TAS is another low-complexity transmission scheme. In this work, we consider three different selection schemes as elaborated below.

1) Criterion 1: In this case, the best antenna is selected to maximize the received SNR at Bob, i.e.,

$$k = \arg \max_{i=1,\cdots,N} |h_{id}|^2, \tag{8}$$

where h_{id} is the i-th element of main channel $\mathbf{h}_M$. It is worth noting that best antenna selection according to the above criterion implies a random antenna selection for the wiretap channel because the main channel is independent of the wiretap channel.

2) Criterion 2: Instead of maximizing the received SNR of the main channel, we now intend to minimize the received SNR of the eavesdropper. As such, the best antenna is selected according to the following criterion:

$$k = \arg \min_{i=1,\cdots,N} |h_{ie}|^2, \tag{9}$$

where h_{ie} is the i-th element of the wiretap channel $\mathbf{h}_W$.

3) Criterion 3: Since the secrecy performance of system depends on the quality of both the main channel and wiretap channel, we now propose the third selection criterion which picks the antenna maximizing the ratio of main channel gain and wiretap channel gain, i.e.,

$$k = \arg \max_{i=1,\cdots,N} \left(\frac{|h_{id}|^2}{|h_{ie}|^2} \right). \tag{10}$$

It is worth pointing out that, this scheme becomes optimal in the high SNR regime.

C. Secrecy Performance Metric

In this work, we focus on the scenario where the source transmits at a constant rate R_S to communicate with the legitimate user. According to [1], perfect secrecy is achievable when R_S is smaller than the secrecy capacity, otherwise, secrecy is compromised. In this case, the secrecy outage probability becomes an appropriate performance metric, which is defined as the probability of the instantaneous secrecy rate

falls below the transmission rate. Hence, the secrecy outage probability can be expressed mathematically as

$$P_{\text{out}}(R_S) = P(C_S < R_S), \tag{11}$$

where C_S is the secrecy capacity defined by the difference of the main channel capacity and the wiretap channel capacity [11]

$$C_S = \begin{cases} \log(1+\gamma_M) - \log(1+\gamma_W) & \gamma_M > \gamma_W, \\ 0 & \gamma_M \leq \gamma_W. \end{cases} \tag{12}$$

III. Secrecy Outage Probability

In this section, we investigate the secrecy outage performance of the considered system. For both transmission schemes, new closed-form expressions for the exact and asymptotic secrecy outage probability are presented. Based on which, the impact of multiple antennas on the secrecy performance are characterized in terms of the secrecy outage diversity order and the secrecy outage array gain.

A. MRT

For the MRT scheme, the secrecy outage probability of the system is given in the following theorem:

Theorem 1: The exact secrecy outage probability of the MRT scheme can be expressed in closed-form as

$$P_{\text{out}}(R_S) = 1 - \frac{2}{\Gamma(mN)} \sum_{k=0}^{N-1} \sum_{p=0}^{k} \frac{\lambda_M \left(k_2\lambda_W\right)^{k-p}}{p! \left(\lambda_M + k_2\lambda_W\right)^{k-p+1}} \times \left(\frac{(k_2-1)m}{k_1\lambda_M\lambda_P}\right)^{\frac{mN+p}{2}} K_{mN-p}\left(2\sqrt{\frac{(k_2-1)m}{k_1\lambda_M\lambda_P}}\right), \tag{13}$$

where $k_1 = \frac{\eta P_S}{N_0}\frac{\theta}{1-\theta}$ and $k_2 = 2^{R_S}$.

Proof: See Appendix A. □

Theorem 1 presents an exact closed-form expression for the secrecy outage probability, which can be efficiently evaluated. However, the expression is too complicated to yield any insights. Motivated by this, we now look into the asymptotic regime, where simple expressions can be obtained.

For the asymptotic high SNR regime, we assume that $\lambda_M \to \infty$ with an arbitrary λ_W. Such a scenario has been widely adopted in the literature, see for instance [2–5]. In practice, this occurs when the quality of the main channel is much better than wiretap channel, i.e., Bob is relatively close to Alice while Eve is far away from Alice or the wiretap channel undergoes severe small-scale and large-scale fading effects.

Theorem 2: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of the MRT scheme can be approximated by

$$P^{\infty}_{\text{out}}(R_S) = \sum_{k=0}^{N} \frac{1}{k!} \frac{\Gamma(mN-k)}{\Gamma(mN)} \left(\frac{m(k_2-1)}{k_1k_2\lambda_W\lambda_P}\right)^k \left(\frac{k_2\lambda_W}{\lambda_M}\right)^N. \tag{14}$$

Proof: We omit the proof due to limited space. □

It is evident from (14) that the system achieves a secrecy diversity order of N. In addition, we observe the intuitive effect of the position of nodes on the secrecy outage probability. For instance, the secrecy outage probability decreases when the PB is close to the source, i.e., large λ_P. It is also easy to see that the high SNR secrecy outage probability $P^{\infty}_{\text{out}}(R_S)$ is a decreasing function with respect to k_1, indicating that increasing the transmit power of the PB is always beneficial.

B. TAS Criterion 1

We now move to the TAS Criterion 1 scheme, and we obtain the following key result:

Theorem 3: The exact secrecy outage probability of TAS Criterion 1 scheme can be expressed in closed-form as

$$P_{\text{out}}(R_S) = 1 - \frac{2}{\Gamma(mN)} \sum_{k=0}^{N-1} \frac{(-1)^k \binom{N}{k+1} \lambda_M}{\lambda_M + k_2\lambda_W(k+1)} \times \left(\frac{m(k+1)(k_2-1)}{k_1\lambda_M\lambda_P}\right)^{\frac{mN}{2}} K_{mN}\left(2\sqrt{\frac{m(k+1)(k_2-1)}{k_1\lambda_M\lambda_P}}\right). \tag{15}$$

Proof: We omit the proof due to limited space. □

While Theorem 3 presents an exact closed-form expression for the secrecy outage probability, the expression is too complicated to gather more insights. As such, we study the asymptotic behavior for the outage performance.

Theorem 4: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of TAS Criterion 1 scheme can be approximated as

$$P^{\infty}_{\text{out}}(R_S) = \sum_{k=0}^{N} \frac{N!}{k!} \frac{\Gamma(mN-k)}{\Gamma(mN)} \left(\frac{m(k_2-1)}{k_1k_2\lambda_W\lambda_P}\right)^k \left(\frac{k_2\lambda_W}{\lambda_M}\right)^N. \tag{16}$$

Proof: We omit the proof due to limited space. □

It is evident from (16) that the system also achieves a secrecy diversity of N. Comparing (14) and (16), we observe that MRT scheme outperforms TAS Criterion 1 scheme. It is not surprising since MRT scheme has access to perfect CSI of $\mathbf{h}_M$, while TAS scheme only utilizes partial knowledge of $\mathbf{h}_M$.

C. TAS Criterion 2

We now consider the TAS Criterion 2 scheme, and we have the following key result:

Theorem 5: The exact secrecy outage probability of TAS Criterion 2 scheme can be expressed in closed-form as

$$P_{\text{out}}(R_S) = 1 - \frac{2}{\Gamma(mN)} \frac{N\lambda_M}{N\lambda_M + k_2\lambda_W} \times \left(\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}\right)^{\frac{mN}{2}} K_{mN}\left(2\sqrt{\frac{m(k_2-1)}{k_1\lambda_M\lambda_P}}\right). \tag{17}$$

Proof: We omit the proof due to limited space. □

Having obtained the exact outage probability of TAS Criterion 2 scheme, we now look into the high SNR regime, and derive a simple analytical approximation for the outage probability of the system.

Theorem 6: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of TAS Criterion 2 scheme can be approximated as

$$P^{\infty}_{\text{out}}(R_S) = \left(\frac{1}{N} + \frac{1}{mN-1}\frac{m(k_2-1)}{k_1k_2\lambda_W\lambda_P}\right)\left(\frac{k_2\lambda_W}{\lambda_M}\right). \tag{18}$$

Proof: We omit the proof due to limited space. □

Different from the previous two cases which achieve a diversity order of N, TAS Criterion 2 scheme only attains unit diversity order. This is also intuitive since TAS Criterion 2 scheme aims to minimize the received SNR of the eavesdropper and the selected antenna serves as a random transmit antenna for the main channel. As such, no secrecy diversity gain can be realized, and increasing the number of antennas N only yields some secrecy array gain.

D. TAS Criterion 3

We now analyze the secrecy outage probability of the system with the TAS Criterion 3 scheme.

Theorem 7: The secrecy outage probability of TAS Criterion 3 scheme can be approximated by

$$P_{\text{out}} \approx \left(\frac{k_2}{k_2 + \frac{\lambda_M}{\lambda_W}} \right)^N. \tag{19}$$

Proof: We omit the proof due to limited space. □

Having obtained the secrecy outage probability of TAS Criterion 3 scheme, we now look into the asymptotic regime.

Theorem 8: In the high SNR regime, i.e., $\lambda_M \to \infty$, the secrecy outage probability of TAS Criterion 3 scheme can be approximated as

$$P_{\text{out}}^{\infty} = \left(\frac{k_2 \lambda_W}{\lambda_M} \right)^N. \tag{20}$$

Proof: We omit the proof due to limited space. □

As expected, the system achieves a secrecy diversity order of N. Recall the high SNR outage probability of the MRT scheme, and noticing that $\sum_{k=0}^{N} \frac{1}{k!} \frac{\Gamma(mN-k)}{\Gamma(mN)} \left(\frac{m(k_2-1)}{k_1 k_2 \lambda_W \lambda_P} \right)^k = 1 + \sum_{k=1}^{N} \frac{1}{k!} \frac{\Gamma(mN-k)}{\Gamma(mN)} \left(\frac{m(k_2-1)}{k_1 k_2 \lambda_W \lambda_P} \right)^k > 1$, we observe that the TAS Criterion 3 scheme outperforms the MRT scheme. This is reasonable since the TAS Criterion 3 scheme has exploited both the CSI of $\mathbf{h}_M$ and $\mathbf{h}_W$, while only the CSI of the $\mathbf{h}_M$ is utilized in the MRT scheme.

E. Comparison of the Proposed Protocols

We now present a more detailed performance comparison for the proposed schemes at the high SNR regime as summarized in Table I. In general, the secrecy performance depends heavily on the available CSI at the source. The more CSI available, the better the secrecy performance.

IV. Numerical Results

In this section, we present numerical results to verify the theoretical expressions. Unless otherwise stated, we set the source transmission rate as $R_S = 1$ bit/s/Hz, the energy conversion efficiency as $\eta = 0.8$ and the time switching ratio as $\theta = 0.5$. The Nakagami-m parameter is set to be $m = 4$, which corresponds to a Rician factor of $K = 3 + \sqrt{12}$. The transmit power of the power beacon to the noise ratio as $\frac{P_S}{N_0} = 10$ dB, the channel variances as $\lambda_P = 1$ and $\lambda_W = 10$. Also, we set $\rho = \frac{P_S}{N_0} \lambda_M$ to denote the average SNR of the main channel.

Fig. 2 plots the secrecy outage probability versus ρ with different N for MRT scheme. As illustrated, the theoretical results are in exact agreement with the Monte Carlo simulations, which demonstrates the accuracy of the theoretical expression. We also see that the high SNR results accurately predict the secrecy diversity order and the secrecy array gain. In addition, we observe that increasing N reduces the secrecy outage probability by improving the secrecy diversity order.

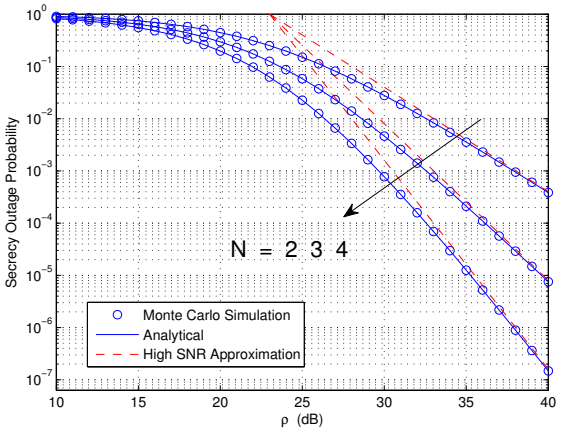

Fig. 2. Secrecy outage probability versus ρ with different N for MRT scheme.

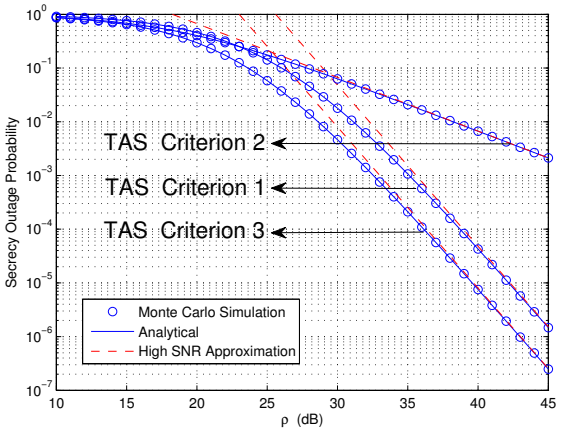

Fig. 3. Secrecy outage probability versus ρ for different TAS schemes with $N = 3$.

Fig. 3 investigates the secrecy outage probability versus ρ for different TAS schemes. Once again, we observe that the analytical curves are in perfect agreement with the Monte Carlo simulation results and the high SNR approximation are sufficiently tight for all curves. We observe that TAS Criterion 2 scheme only attains unit diversity order and TAS Criterion 3 scheme performs best.

V. Conclusion

In this paper, we have investigated the secrecy performance of the wirelessly powered wiretap channels. For the MRT and TAS schemes, the exact analytical expressions and asymptotic approximations are presented, which facilitate the extraction of key insights of the achievable secrecy performance. The findings of the paper suggest that, with CSI of the main

TABLE I. Comparison of the proposed schemes

Scheme	CSI requirement	Secrecy diversity order	Secrecy outage performance
MRT	$\mathbf{h}_M$	N	Second best
TAS Criterion 1	Index of the entry of $\mathbf{h}_M$	N	Third best
TAS Criterion 2	Index of the entry of $\mathbf{h}_W$	1	Worst
TAS Criterion 3	$\mathbf{h}_M$ and $\mathbf{h}_W$	N	Best

channel, the system can achieve substantial secrecy diversity gain. On the other hand, without the CSI of the main channel, no diversity gain can be attained, which indicates the critical importance of CSI in the design of practical systems.

Appendix A
Proof of Theorem 1

We start by expressing the SNR given in (6) and (7) as

$$\gamma_M = k_1 y_{h_P} y_{h_M}, \quad \text{and} \quad \gamma_W = k_1 y_{h_P} y_{h_W}, \tag{21}$$

where $k_1 = \frac{\eta P_S}{N_0}\frac{\theta}{1-\theta}$, $y_{h_P} = ||\mathbf{h}_P||^2$, $y_{h_M} = ||\mathbf{h}_M||^2$ and $y_{h_W} = \frac{|\mathbf{h}_W^T \mathbf{h}_M^{'}|^2}{||\mathbf{h}_M||^2}$. It is straightforward to show that the probability density function (pdf) of y_{h_P} follows a gamma distribution with shape parameter mN and scale parameter λ_P/m given by [12]

$$f_{y_{h_P}}(x) = \frac{1}{\Gamma(mN)}\left(\frac{m}{\lambda_P}\right)^{mN} x^{mN-1} e^{-\frac{m}{\lambda_P}x}, \tag{22}$$

and the pdf of y_{h_M} follows a chi-square distribution with $2N$ degrees of freedom given by [13]

$$f_{y_{h_M}}(x) = \frac{x^{N-1}}{\lambda_M^N \Gamma(N)} e^{-\frac{x}{\lambda_M}}. \tag{23}$$

In addition, according to [14], y_{h_W} follows an exponential distribution with pdf

$$f_{y_{h_W}}(x) = \frac{1}{\lambda_W} e^{-\frac{x}{\lambda_W}}, \tag{24}$$

and we claim that y_{h_W} and y_{h_M} are independent. As such, the secrecy outage probability can be written as

$$P_{\text{out}}(R_S) = 1 - P\left(\frac{1 + k_1 y_{h_P} y_{h_M}}{1 + k_1 y_{h_P} y_{h_W}} \geq k_2\right), \tag{25}$$

where $k_2 = 2^{R_S}$. Conditioned on y_{h_P} and y_{h_W}, with the help of [9, Eq. (3.351.2)], we obtain

$$\begin{aligned} P_{\text{out}}(R_S) &= 1 - \int_{\frac{k_2-1}{k_1 y_{h_P}} + k_2 y_{h_W}}^{\infty} \frac{x^{N-1}}{\lambda_M^N \Gamma(N)} e^{-\frac{x}{\lambda_M}} \mathrm{dx} \\ &= 1 - e^{-\frac{k_2-1}{k_1 \lambda_M y_{h_P}} - \frac{k_2 y_{h_W}}{\lambda_M}} \sum_{k=0}^{N-1} \frac{1}{k!}\left(\frac{k_2-1}{k_1 \lambda_M y_{h_P}} + \frac{k_2 y_{h_W}}{\lambda_M}\right)^k. \end{aligned} \tag{26}$$

By applying the binomial expansion $(x_1 + x_2)^n = \sum_{k=0}^{n} \binom{n}{k} {x_1}^k {x_2}^{n-k}$, (26) can be further expressed as

$$\begin{aligned} P_{\text{out}}(R_S) = 1 - \sum_{k=0}^{N-1} \sum_{p=0}^{k} \frac{1}{p!(k-p)!} \times \\ e^{-\frac{k_2-1}{k_1 \lambda_M y_{h_P}}} \left(\frac{k_2-1}{k_1 \lambda_M y_{h_P}}\right)^p e^{-\frac{k_2 y_{h_W}}{\lambda_M}} \left(\frac{k_2 y_{h_W}}{\lambda_M}\right)^{k-p}. \end{aligned} \tag{27}$$

Noticing that the random variable y_{h_P} is decoupled with y_{h_W}, the execration can be taken separately. Hence, with the help of [9, Eq. (3.471.9)], we obtain

$$\begin{aligned} &\int_0^{\infty} e^{-\frac{k_2-1}{k_1 \lambda_M x}} \left(\frac{k_2-1}{k_1 \lambda_M x}\right)^p \frac{x^{mN-1}}{\Gamma(mN)} \left(\frac{m}{\lambda_P}\right)^{mN} e^{-\frac{m}{\lambda_P}x} \mathrm{dx} \\ &= \frac{2}{\Gamma(mN)} \left(\frac{(k_2-1)m}{k_1 \lambda_M \lambda_P}\right)^{\frac{mN+p}{2}} K_{mN-p}\left(2\sqrt{\frac{(k_2-1)m}{k_1 \lambda_M \lambda_P}}\right). \end{aligned} \tag{28}$$

Similarly, invoking [9, Eq. (3.326.2)], we have

$$\int_0^{\infty} e^{-\frac{k_2 x}{\lambda_M}} \left(\frac{k_2 x}{\lambda_M}\right)^{k-p} \frac{e^{-\frac{x}{\lambda_W}}}{\lambda_W} \mathrm{dx} = \frac{(k-p)! \lambda_M \left(k_2 \lambda_W\right)^{k-p}}{\left(\lambda_M + k_2 \lambda_W\right)^{k-p+1}}. \tag{29}$$

To this end, pulling everything together yields the desired result.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[2] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[3] X. Chen, C. Zhong, C. Yuen, and H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40–46, Dec. 2015.

[4] S. Hessien, F. S. Al-Qahtani, R. M. Radaydeh, C. Zhong, and H. Alnuweiri, "On the secrecy enhancement with low-complexity large-scale transmit selection in MIMO generalized composite fading," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 429–432, Aug. 2015.

[5] F. S. Al-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.

[6] K. Huang and V. K. N. Lau, "Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 902–912, Feb. 2014.

[7] C. Zhong, X. Chen, Z. Zhang, and G. K. Karagiannidis, "Wireless-powered communications: Performance analysis and optimization," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5178–5190, Dec. 2015.

[8] C. Zhong, G. Zheng, Z. Zhang, and G. K. Karagiannidis, "Optimum wirelessly powered relaying," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1728–1732, Oct. 2015.

[9] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products,* 6th Ed.. San Diago: Academic Press, 2000.

[10] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, July 2013.

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

[12] A. M. Magableh and M. M. Matalgah, "Capacity of SIMO systems over non-identically independent Nakagami-m channels," *Proc. IEEE Sarnoff Symposium*, pp. 1–5, April 2007.

[13] M. K. Simon and M. S. Alouini, "Digital Communication over Fading Channels: A Unified Approach to Performance Analysis," Hoboken, NJ: Wiley, 2000.

[14] A. Shah and A. M. Haimovich, "Performance analysis of maximal ratio combining and comparison with optimum combining for mobile radio communications with cochannel interference," *IEEE Trans. Veh. Technol.*, vol. 49, no. 4, pp. 1454–1463, July 2000.