Secure Energy Harvesting Relay Networks with Unreliable Backhaul Connections

Yin, C., Nguyen, H. T., Kundu, C., Kaleem , Z., Garcia-Palacios, F., & Duong, Q. (2018). Secure Energy Harvesting Relay Networks with Unreliable Backhaul Connections. *IEEE Access*, 1-9. Advance online publication. https://doi.org/10.1109/ACCESS.2018.2794507

Published in:
IEEE Access

Document Version:
Publisher's PDF, also known as Version of record

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
Copyright 2018 the authors.
This is an open access article published under a Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution and reproduction in any medium, provided the author and source are cited.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Open Access
This research has been made openly available by Queen's academics and its Open Research team. We would love to hear how access to this research benefits you. – Share your feedback with us: http://go.qub.ac.uk/oa-feedback

Download date:10. Jul. 2025

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2794507, IEEE Access

Secure Energy Harvesting Relay Networks with Unreliable Backhaul Connections

Cheng Yin, *Student Member, IEEE,* Huy T. Nguyen, *Student Member, IEEE,* Chinmoy Kundu, *Member, IEEE,* Zeeshan Kaleem, *Member, IEEE,* Emiliano Garcia-Palacios, *Member, IEEE* , and Trung Q. Duong *Senior Member, IEEE,*

***Abstract*—Wireless backhaul is a cost-effective and flexible alternative to wired backhaul, yet it suffers from unreliability. This paper studies the secrecy performance of a relay network with such unreliable wireless backhaul. Bernoulli process is adopted to model the wireless backhaul reliability. In the network, a relay employing time-switching-based radio frequency harvesting technique aids in forwarding the signal from the best transmitter. An eavesdropper, which is able to wiretap signals from both the transmitter and the relay, uses selection combining to maximize its received signal-to-noise ratio. Analytical expressions for secrecy outage probability, ergodic secrecy rate and non-zero achievable secrecy rate are derived, which can reveal the effect of the number of transmitters and backhaul reliability on the system performance. Furthermore, for the first time the impact of energy harvesting time fraction upon secrecy performances under unreliable backhaul is presented.**

***Index Terms*—Energy harvesting, ergodic secrecy rate, secrecy outage probability, transmitter selection, unreliable backhaul.**

I. Introduction

A high dense network is envisaged in the near future where multiple backhaul connections have to be provided. Conventional wired backhaul technologies such as copper, optical fibre and line-of-sight (LOS) microwave can ensure reliability and high data rate, but the cost for their deployment and maintenance is relatively high [1] [2]. In contrast, wireless backhaul has been proven to be a cost-effective and flexible alternative, yet not without its drawback. The links in a wireless backhaul solution are not as reliable due to non-LOS propagation and channel fading [3]. However, with scenarios such as smart cities, smart grids and the Internet-of-Things gaining momentum, there is no doubt that future networks will be dense and heterogeneous [4] and that the flexible, cost efficient wireless backhaul is an attractive proposition despite being unreliable. As such, the security and privacy issue for future wireless networks is very crucial [5].

In this context, the use of relays is also attractive as they can extend the coverage and enhance the overall system performance [6]–[11]. There are two main schemes, namely amplify-and-forward (AF) and decode-and-forward (DF) [12]. In AF schemes, the relay amplifies the received message and then forwards it to the receiver, thus requires less power because there is no decoding or quantizing at the relay. The drawback is that the interference is also amplified. In DF schemes, the relay decodes the source message in one block and transmits the decoded message in the following. Consequently, a relay network operating in DF schemes has better performance thanks to lower interference, which motivates us to consider cooperative DF relays in this work. To overcome the need for more power to operate as a result of its complexity, we exploit alternative ways of harvesting energy for the relays.

In recent years, radio frequency (RF) energy harvesting (EH) has been presented as a promising environmental friendly approach. RF signals with wireless information and energy are transmitted so that the nodes can receive the harvested energy to forward or process information [13] [14]. In [15], the power beacon provides wireless energy for relay nodes to stay active. In [16], a cooperative energy harvesting network with time switching (TS) protocol at the relay is investigated. In this work, the relay will harvest energy from a selected transmitter during an energy harvesting period, receive the information from the backhaul and forward the information to the destination.

For a more complete study one also needs to take into consideration the inherent challenges of security in future wireless communication networks. Due to the broadcast nature, information is vulnerable to eavesdropping and hostile attacks [16]–[19]. The traditional way is deploying cryptographic techniques which are used at higher-layers on the condition that there is no error at the physical layer, despite this consumes a hugh amount of energy for encrypting, decrypting data and burdening the protocol stack. In recent years, physical layer security (PLS) has become increasingly popular to tackle significant concerns in wireless communications. The principle of PLS is that the randomness of the wireless channels can be exploited to keep the information confidential from eavesdroppers. Some research has investigated the system performance in the presence of an eavesdropper [16], [20]–[30]. In this work, we consider an eavesdropper that can wiretap the information from the transmitters and the relay.

These research studies do not investigate the effect of the unreliability of wireless backhaul links on the system performance. For instance, in [21], the authors considered EH, relay networks and PLS in a wireless network with Rayleigh fading,

Cheng Yin, Chinmoy Kundu, Trung Q. Duong and Emiliano Garcia-Palacios are with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Northern Ireland, U.K., e-mail: {cyin01, c.kundu, trung.q.duong, }@qub.ac.uk, and e.garcia@ee.qub.ac.uk.

Huy T. Nguyen is with the Inje University, South Korea, e-mail: huynguyencse@gmail.com.

Z. Kaleem is with COMSATS Institute of Information Technology, Wah, Pakistan, e-mail: zeeshankaleem@gmail.com

The work was supported in part by U.K. Engineering and Physical Sciences Research Council under Grant EP/P019374/1 and by the Royal Society-SERB Newton International Fellowship under Grant NF151345.

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2794507, IEEE Access

without considering the impact of the unreliable backhaul on the system performance. However, there has been research into this important role of wireless backhaul. A cooperative wireless system with unreliable backhaul is investigated in [3], [31]–[33]. Moreover, the system performance is shown to decrease because of the unreliable wireless backhaul links [31]. Related research in [31] and [32] is extended by considering an energy harvesting relay to enhance coverage and PLS to keep information confidential from an eavesdropper. In [31] and [32], a control unit (CU) sends a message to transmitters via unreliable backhaul links. When the information is transmitted successfully, it is forwarded to the receiver. In addition, selection combing (SC) is used at the receiver to increase the throughput and maximize the signal-to-noise ratio (SNR) in [32]. However, neither relaying nor security is considered in these studies.

In [3], the secrecy performance of finite-sized cooperative single-carrier systems with unreliable backhaul connections is investigated. In [34], the secrecy performance of cooperative single-carrier systems has been derived under the unreliable backhaul. Closed-form expressions were derived to study the secrecy outage probability, ergodic secrecy rate and the probability of non-zero achievable secrecy rate.

Different from all the aforementioned work, in this paper, we consider unreliable backhaul in EH relay networks where the terminals are under realistic constraints that their batteries are limited. Our work presents a more complete model by including an EH relay to extend coverage and to show the impact of EH time fraction upon secrecy for the first time.

Our main contributions are summarized as below:

- We investigate the impact of unreliable backhaul on the secrecy performance of EH relay networks with transmitter selection.
- We provide analytical expressions to evaluate the performances of secrecy outage probability, non-zero achievable secrecy rate and ergodic secrecy rate.
- We investigate the effect of the number of transmitters, EH time-fraction ratio, and wireless backhaul reliability on the secrecy performance is investigated.

The remainder of the paper is organized as follows. System and channel models are described in Section II. Derivation of the SNR distributions is obtained in the Section III. Secrecy performance analysis is carried out in the Section IV, while numerical results are presented in the Section V. Finally, the paper is concluded in the Section VI.

Notation: $\mathbb{P}[\cdot]$ is the probability of occurrence of an event. For a random variable X, $\mathbb{E}_X[\cdot]$ denotes expectation or mean of X, $F_X(\cdot)$ denotes its cumulative distribution function (CDF) and $f_X(\cdot)$ denotes the corresponding probability density function (PDF). $(x)^+ \triangleq \max(0,x)$, and $\max(\cdot)$ and $\min(\cdot)$ denote the maximum and minimum of their arguments, respectively. λ_{XY} denotes inverse of the average SNR of the arbitrary link $X-Y$.

II. System and Channel Models

A cooperative EH network, consisting of a macro base station S connected to K small-cell transmitters, $TX_{\{1,\cdots,K\}}$, via unreliable backhaul links, a relay, R, and a destination, D, in presence of an eavesdropper, E, is considered as shown in Fig. 1. The best transmitter is selected to transfer its message to D with the help of R while E attempts to wiretap information transmitted from both the transmitter and R. The relay is assumed to be operating in half-duplex DF and constrained by the amount of radio energy it harvests from the selected transmitter within the time allocated to it. Time switching (TS) based EH mechanism is considered as shown in Fig. 2 where α, $0<\alpha<1$, is the fraction of the total time period T for the harvesting radio energy.

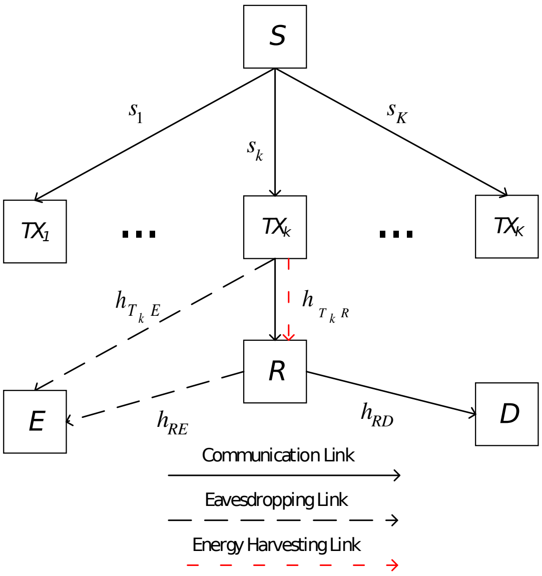

Fig. 1: System Model

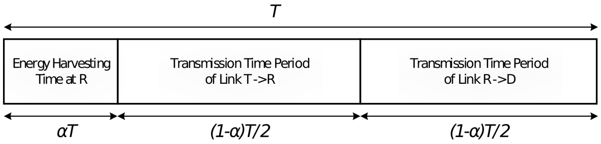
T
Energy Harvesting Time at R
Transmission Time Period of Link T->R
Transmission Time Period of Link R->D
αT
(1-α)T/2
(1-α)T/2

Fig. 2: Time Switching Based Protocol

Reliability of the k^{th} Backhaul is modeled as a Bernoulli process $\mathbb{I}_k$ with success probability s_k where $\mathbb{P}(\mathbb{I}_{k^*}=1)=s_k$ and $\mathbb{P}(\mathbb{I}_{k^*}=0)=1-s_k$. This indicates that the TX_k is participating in the transmission if the message is successfully delivered over its dedicated backhaul with probability s_k whereas it defers its transmission with probability $1-s_k$. All the channels are assumed to undergo independent and identically distributed (i.i.d) Rayleigh fading. It is also assumed that transmitters and the receiver are equipped with a single antenna. The best transmitter (k^*) is the transmitter for which the received SNR at R is maximum, i.e.,

$$k^* = \arg\max_{1\leq k\leq K} \mathrm{SNR}_{T_k R}. \tag{1}$$

The eavesdropper combines signals from TK_{k^*} and R using SC to maximize its received SNR.

In the first hop, the received signal at R and E are of the form

$$y_R = \sqrt{P_T} h_{T_{k^*}R} \mathbb{I}_{k^*} x + z, \tag{2}$$

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

where $h_{T_{k^*}R}$ is the channel coefficient of the link $TX_{k^*}-R$, x is the unit power transmitted symbol and P_T is the transmitted power by TX_{k^*}, z is the complex additive white Gaussian noise (AWGN) at R with zero mean and variance σ, i.e., $z \sim CN(0, \sigma)$. Received signal at E can be obtained by simply replacing R by E in (2).

In the second hop, the received signal at D and E are of the form

$$y_D = \sqrt{P_R} h_{RD} x + z, \tag{3}$$

where P_R is the transmitted power by R which is harvested in the first time slot, h_{RD} is the channel coefficient of the link $R-D$. Received signal at E can be obtained by simply replacing D with E in (3). It is to be noted here that receivers are assumed to be affected by the same amount of noise power.

A. Harvested Power

Considering TS policy based EH, the harvested energy at R can be obtained as [13]

$$E_R = \eta \alpha T P_T |h_{T_{k^*}R}|^2 \mathbb{I}_{k^*} \tag{4}$$

where η is the EH efficiency and $0 < \eta < 1$. Corresponding harvested power can be obtained as

$$P_R = \xi P_T |h_{T_{k^*}R}|^2 \mathbb{I}_{k^*} \tag{5}$$

where $\xi = \frac{2\eta\alpha}{(1-\alpha)}$.

III. SNR DISTRIBUTIONS

Before the secrecy performances are derived in the next section, this section finds the distributions of the SNRs necessary for the derivation.

A. Distribution of the link $T_{k^*} - R$.

According to the transmitter selection rule, the SNR of the best link $T_{k^*} - R$ can be written as

$$SNR_{T_{k^*}R} = \max_{k=1,\ldots,K} \frac{P_T |h_{T_k R}|^2 \mathbb{I}_k}{\sigma^2}. \tag{6}$$

Corresponding CDF can be obtained as

$$F_{\gamma_{M1}}(x) = 1 + \sum_{k=1}^{K} (-1)^k \binom{K}{k} s^k \exp\left(-\lambda_{TR} \frac{kx}{\gamma_M}\right), \tag{7}$$

where $\gamma_M = \frac{P_T}{\sigma^2}$.

Proof: The proof is given in Appendix A. ■

B. Distribution of the link $R - D$.

SNR of the link $R-D$ can be written in the form of

$$SNR_{RD} = \frac{P_R |h_{RD}|^2}{\sigma^2}, \tag{8}$$

where P_R is the harvested power in the first time slot as in (5). SNR of the link $R-E$ can be obtained just by replacing D with E in (8). The corresponding CDF is derived as

$$F_{\gamma_{M2}}(x) = 1 + \sum_{k=1}^{K} (-1)^k s^k \binom{K}{k} 2\sqrt{\frac{\lambda_{TR}\lambda_{RD} kx}{\gamma_M \xi}} \times \mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD} kx}{\gamma_M \xi}}\right), \tag{9}$$

where $\mathcal{K}_v(z)$ is the modified Bessel function of the second kind.

Proof: The proof is given in Appendix B. ■

C. Distribution of the end-to-end link $T_{k^*} - D$.

As R follows DF relaying protocol, the end to end SNR at D is expressed as

$$SNR_{T_{k^*}D} = \min(SNR_{T_{k^*}R}, SNR_{RD}). \tag{10}$$

The CDF of the link can be expressed as

$$\begin{aligned} F_{\gamma_{TD}}(x) &= 1 - (1 - F_{\gamma_{M1}}(x))(1 - F_{\gamma_{M2}}(x)) \\ &= 1 - \sum_{k=1}^{K} (-1)^k \binom{K}{k} s^k \exp\left(-\lambda_{TR}\frac{kx}{\gamma_M}\right) \sum_{i=1}^{K} (-1)^i s^i \binom{K}{i} \\ &\times 2\sqrt{\frac{\lambda_{TR}\lambda_{RD} ix}{\gamma_M \xi}} \mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD} ix}{\gamma_M \xi}}\right). \end{aligned} \tag{11}$$

D. Distribution of the link $T_{k^*} - E$.

The SNR of the link $T_{k^*} - E$ is given by

$$SNR_{T_{k^*}E} = \frac{P_T |h_{T_{k^*}E}|^2 \mathbb{I}_{k^*}}{\sigma^2}. \tag{12}$$

Hence, corresponding CDF can be obtained following Appendix A as

$$F_{\gamma_{E1}}(x) = 1 - s \exp\left(-\lambda_{TE}\frac{x}{\gamma_M}\right). \tag{13}$$

E. Distribution of the link $R - E$.

The CDF of the link $R-E$ can be obtained as of the link $R-D$ in (9) as

$$F_{\gamma_{E2}}(x) = 1 + \sum_{k=1}^{K} (-1)^k s^k \binom{K}{k} 2\sqrt{\frac{\lambda_{TR}\lambda_{RE} kx}{\gamma_M \xi}} \times \mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RE} kx}{\gamma_M \xi}}\right). \tag{14}$$

F. Distribution of the SNR at E.

As E follows SC protocol, the SNR at E can be expressed as

$$SNR_E = \max(SNR_{T_{k^*}E}, SNR_{RE}). \tag{15}$$

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2794507, IEEE Access

The corresponding CDF can be evaluated using (13) and (14) as

$$\begin{aligned}
&F_{\gamma_E}\left(x\right)=F_{\gamma_{E1}}\left(x\right)F_{\gamma_{E2}}\left(x\right)\\
&=1+\sum_{k=1}^{K}(-1)^k\binom{K}{k}s^k2\sqrt{\frac{\lambda_{TR}\lambda_{RE}kx}{\gamma_M\xi}}\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RE}kx}{\gamma_M\xi}}\right)\\
&-s\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right)-s\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right)\sum_{i=1}^{K}(-1)^i\binom{K}{i}s^i\\
&\times 2\sqrt{\frac{\lambda_{TR}\lambda_{RE}ix}{\gamma_M\xi}}
\end{aligned} \tag{16}$$

By differentiating (16), the PDF of the SNR at E is expressed as

$$\begin{aligned}
&f_{\gamma_E}\left(x\right)=-\sum_{i=1}^{K}(-1)^is^i\binom{K}{i}2\frac{i\lambda_{TR}\lambda_{RE}}{\gamma_M\xi}\mathcal{K}_0\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RE}ix}{\gamma_M\xi}}\right)\\
&+\frac{\lambda_{TE}s}{\gamma_M}\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right)+s\sum_{j=1}^{K}(-1)^js^j\binom{K}{j}2\sqrt{\frac{\lambda_{TR}\lambda_{\mathsf{RE}}j}{\gamma_M\xi}}\\
&\times\frac{\lambda_{TE}}{\gamma_M}\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{\mathsf{RE}}jx}{\gamma_M\xi}}\right)\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right)x^{\frac{1}{2}}+s\sum_{k=1}^{K}\\
&\times(-1)^ks^k\binom{K}{k}\frac{2\lambda_{RE}k\lambda_{TR}}{\gamma_M\xi}\mathcal{K}_0\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RE}kx}{\gamma_M\xi}}\right)\\
&\times\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right).
\end{aligned} \tag{17}$$

In the above equation, the first derivative of the modified Bessel function of the second kind is utilized as follows

$$\frac{\partial\mathcal{K}_v\left(z\right)}{\partial z}=-\mathcal{K}_{v-1}\left(z\right)-\frac{v}{z}\mathcal{K}_v\left(z\right). \tag{18}$$

IV. Secrecy Performance Analysis

This section derives the performances of secrecy outage probability, non-zero achievable secrecy rate and ergodic secrecy rate utilizing the SNR distributions obtained in the previous section. Towards deriving those performances, the secrecy rate of the system is required to be defined first, which is given by

$$C_S=\frac{1}{2}\left[\log_2(1+SNR_{T_k^*\to D})-\log_2(1+SNR_E)\right]^+, \tag{19}$$

where $[x]^+=\max(x,0)$.

A. Secrecy outage probability

The secrecy outage probability is defined as the probability that the secrecy rate falls below a certain threshold θ, i.e.,

$$\begin{aligned}
\mathcal{P}_{out}(\theta)&=Pr(C_S<\theta)\\
&=\int_0^\infty F_{T_k*D}\left(2^{2\theta}(1+x)-1\right)f_E\left(x\right)dx,
\end{aligned} \tag{20}$$

Substitute (11) and (17) into (20), the expression for secrecy outage probability can be obtain in (B.2) as shown in the Appendix C.

B. Probability of non-zero secrecy rate

The probability of non-zero secrecy rate is the probability that secrecy rate is more than zero, or another way $SNR_{T_{k^*}D}$ is higher than SNR_E. The probability of none-zero secrecy rate can be obtained as [35]

$$\begin{aligned}
Pr(C_S>0)&=1-\mathcal{P}_{out}(0)\\
&=1-\int_0^\infty F_{SNR_{T_k^*\to D}}\left(x\right)f_{SNR_E}\left(x\right)dx,
\end{aligned} \tag{21}$$

Using (11) and (17), it can be evaluated in (B.6) as shown in the Appendix D.

C. Ergodic secrecy rate

The ergodic secrecy rate is defined as the average secrecy rate averaged over all the SNR distributions. Ergodic secrecy rate (bits/s/Hz) is expressed as [35]

$$\mathcal{C}_{erg}=\frac{1}{2\ln(2)}\int_0^\infty\frac{F_{SNR_E}\left(x\right)}{1+x}[1-F_{SNR_{T_k^*\to D}}\left(x\right)]dx \tag{22}$$

Substitute (11) and (16) into (22), ergodic secrecy rate can be evaluated as in (B.7) as shown in the Appendix E.

V. Numerical results

In this section, numerical results along with simulations are shown for the analyses carried out on the proposed system. The threshold of secrecy outage probability is fixed at $\theta = 1$ bits/s/Hz. It is assumed that the location of the nodes in Cartesian coordinate system respectively are TX_k = (0, 0), $\forall k$, R =(0.8, 0), D =(1, 0), E =(1, -4) [36]. Hence, the distance between two nodes can be found as d_{AB}=$\sqrt{(x_A-x_B)^2+(y_A-y_B)^2}$, where A and B have the co-ordinates (x_A, y_A) and (x_B, y_B) and $A, B = \{T, R, D, E\}$. It is assumed that average SNR of each link is dependent on the path loss as $1/\lambda_X = 1/d_X^{pl}$, where, pl is the path loss exponent. Unless otherwise specified, $pl = 4$ and $\eta = 0.5$ is assumed. In figures, "sim" represents the simulation results, and "ana" represents the analytical results.

A. Effect of number of transmitters, reliability of backhaul and EH time on secrecy outage probability

In Fig. 3, secrecy outage probability versus γ_M is plotted by increasing the number of transmitters from $K = 1$ to 3. The parameters, $s = 0.98$, and $\alpha = 0.2$ are assumed. As the number of transmitters increases, secrecy outage probability decreases. This is because of the increased diversity with increased number of transmitters. It can also be seen that as γ_M increases, secrecy outage probability initially decreases, however, becomes saturated at a fixed value for a given K.

In Fig. 4, secrecy outage probability versus γ_M is plotted by increasing the reliability of the backhaul as $s = 0.8, 0.9, 0.98$ for $K = 3$. The parameters $\alpha = 0.2$ is assumed. It can observed that if the system has more reliable backhaul, it performs better.

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2794507, IEEE Access

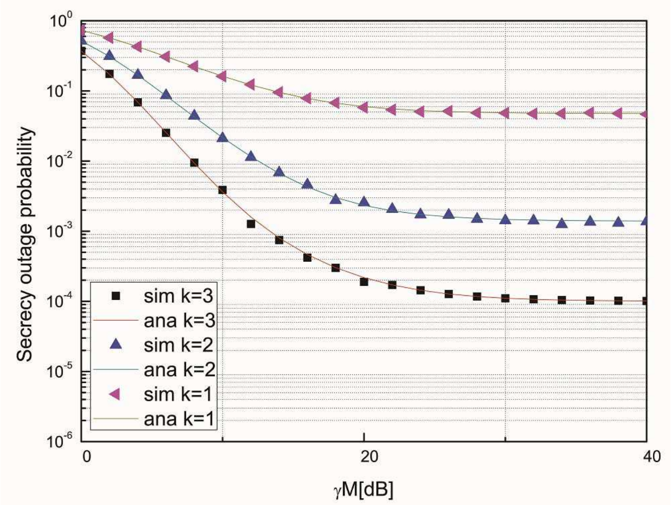

Fig. 3: Secrecy outage probability with different number of transmitters at a fixed backhaul reliability.

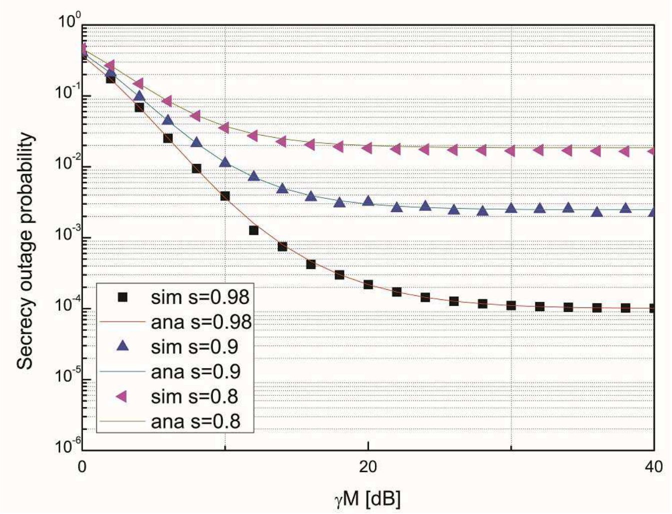

Fig. 4: Secrecy outage probability with different backhaul reliability at a fixed number of transmitters.

In Fig. 5, secrecy outage probability versus time fraction, α, allowed to do the EH is shown at a specific s=0.98. It is observed that the secrecy outage probability tends to get higher when α is too low or too high. It has a convex nature with α. This is because when the EH time is too high, the relay does not have sufficient time to transmit the signal as a result, received power decreases, and when it is too low, so little energy is harvested that transmit power decreases. In both the cases, the secrecy outage probability will be extremely high. It can be noticed that with the number of transmitters varying, the curves show the same trend and has the same optimal point obtained at $\alpha = 0.2$. This shows that the number of transmitters has no effect on the optimal EH time.

B. Effect of number of transmitters, reliability of backhaul and EH time on ergodic secrecy rate

Fig. 6, Fig. 7 and Fig. 8 depict the effect of the number of transmitters, backhaul reliability, EH time fraction on the ergodic secrecy rate as shown in the corresponding figures Fig. 3, Fig. 4 and Fig. 5, respectively, on the secrecy outage probability. Parameters are the same in the corresponding figures of the ergodic secrecy rate and secrecy outage probability. Effect of number of transmitters, reliability of backhaul and EH time is complementary on ergodic secrecy rate and secrecy outage probability. When secrecy outage probability decreases, the ergodic secrecy rate would increase. Observations from these figures are as follows: ergodic secrecy rate increases initially with γ_M, however, saturates afterwards, as K increases, ergodic secrecy rate also increases, ergodic secrecy rate is concave in nature with α, as reliability of the backhaul increases, ergodic secrecy rate also increases.

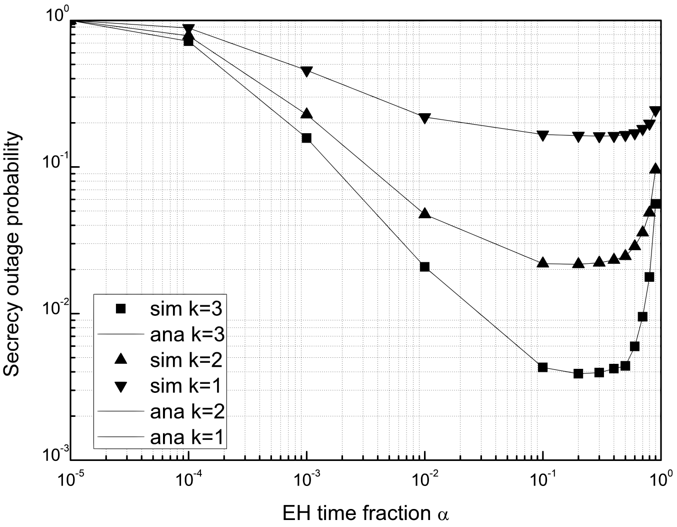

Fig. 5: Secrecy outage probability plotted as a function of α at a fixed backhaul reliability.

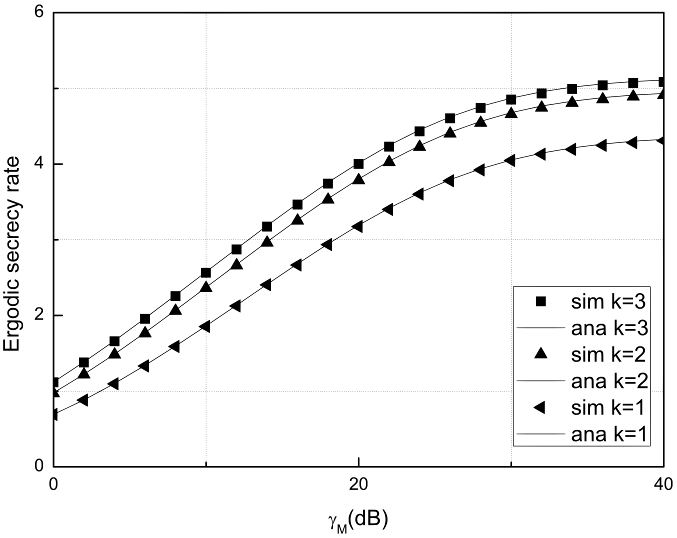

Fig. 6: Ergodic secrecy rate with different number of transmitters at fixed backhaul reliability.

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

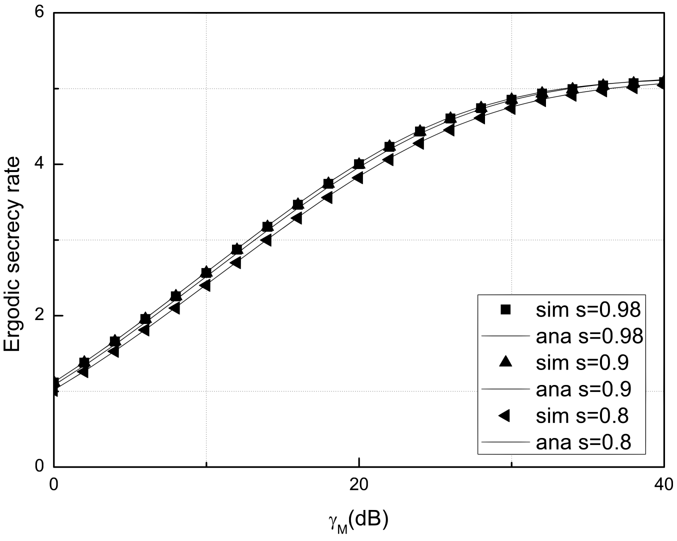

Fig. 7: Ergodic secrecy rate with different backhaul reliability at a fixed number of transmitters.

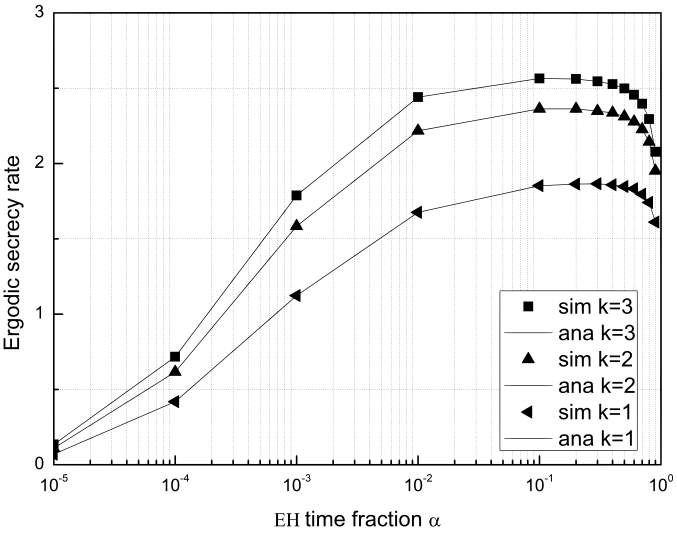

Fig. 8: Ergodic secrecy rate plotted as a function of α at a fixed backhaul reliability.

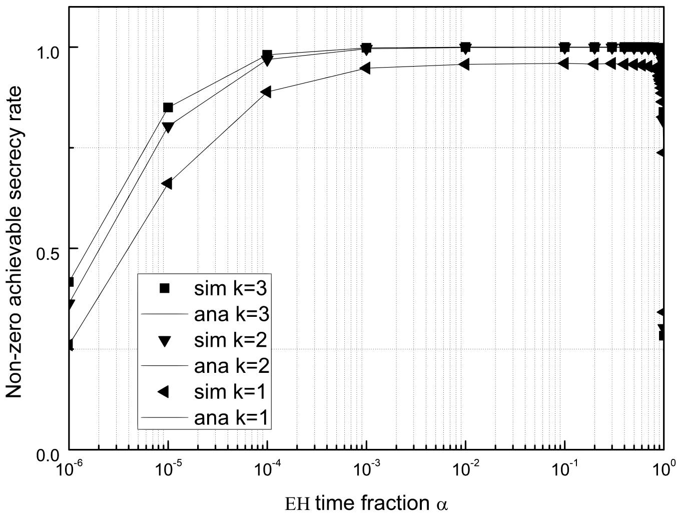

Fig. 9: Probability of non-zero achievable secrecy rate plotted as a function of α at a fixed backhaul reliability.

C. Effect of number of transmitters, reliability of backhaul and EH time on non-zero secrecy rate

Fig. 9 shows the same performances as of secrecy outage probability and ergodic secrecy rate with the same parameters, correspondingly. The observations are similar in all the cases.

In the figure, simulation results match well with the numerical results, thus, validating the analysis presented in the paper.

VI. Conclusion

This paper investigated the effect of unreliable backhaul on the secrecy of an energy harvesting relay network with transmitter selection. Three performance metrics, i.e., secrecy outage probability, non-zero achievable secrecy rate and ergodic secrecy rate, were derived under independent Rayleigh fading channels. Results showed that the increase in the backhaul reliability and the number of transmitters improve the system performance. It was also shown that energy harvesting time fraction has a huge impact on the system performance, hence, should be optimally designed.

Appendix A

As individual links are i.i.d Rayleigh distributed, corresponding SNRs are exponentially distributed. Assuming success probability s for each link i.e., $s_k = s,\ \forall k$, distribution of SNR_{T_kR} can be written as (avoiding the subscript k hereafter as i.i.d links)

$$f_{|h_{TR}|^2\mathbb{I}}(t) = (1-s)\delta(t) + s\lambda_{TR}\exp(-\lambda_{TR}t), \tag{A.1}$$

where $\delta(t)$ is the Dirac delta function and $1/\lambda_{TR}$ is the average SNR of the corresponding link. The corresponding CDF can be written as

$$\begin{aligned} F_{|h_{TR}|^2\mathbb{I}}(t) &= \int_0^t (1-s)\delta(t) + s\lambda_{TR}\exp(-\lambda_{TR}t)dt \\ &= 1 - s\exp\left(-\lambda_{TR}\frac{t}{\gamma_M}\right) \end{aligned} \tag{A.2}$$

Now the CDF of $SNR_{T_{k^*}R} = \max_{k=1,\dots,K} \gamma_M h_{T_kR}\mathbb{I}_k$ is

$$\begin{aligned} F_{\gamma_{M1}}(t) &= \left(1 - s\exp\left(-\lambda_{TR}\frac{t}{\gamma_M}\right)\right)^K \\ &= 1 + \sum_{k=1}^{K}(-1)^k\binom{K}{k}s^k\exp\left(-\lambda_{TR}\frac{kt}{\gamma_M}\right) \end{aligned} \tag{A.3}$$

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2794507, IEEE Access

APPENDIX B

The CDF of SNR_{RD} can be found from the definition assigning auxiliary variable t to $|h_{RD}|^2$ as

$$\begin{aligned}
&F_{\gamma_{M2}}(x) = \mathbb{P}\left[\xi\gamma_M|h_{T_{k^*}R}|^2|h_{RD}|^2\mathbb{I}_{k^*} \leq x\right] \\
&= \mathbb{P}\left[\gamma_M|h_{T_{k^*}R}|^2\mathbb{I}_{k^*} < \frac{x}{\xi t}\right] \\
&= \int_0^\infty \left(1 + \sum_{k=1}^{K}(-1)^k \binom{K}{k} s^k \exp\left(-\lambda_{TR} k \frac{x}{\gamma_M \xi t}\right)\right) f(t)dt \\
&= 1 + \sum_{k=1}^{K}(-1)^k s^k \binom{K}{k} 2\sqrt{\frac{\lambda_{TR}\lambda_{RD}kx}{\gamma_M\xi}} \\
&\times \mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD}kx}{\gamma_M\xi}}\right) \qquad \text{(B.1)}
\end{aligned}$$

The integral can be solved according to [37, Eq. (3.324.1)].

APPENDIX C

The expression for the secrecy outage probability is shown in (B.2). The integrals $J1$ and $J4$ can be written in the form of

$$\int_0^\infty \exp(ax)\mathcal{K}_0\left(\sqrt{a_0 x}\right)\mathcal{K}_1\left(\sqrt{b_0 x + d_o}\right)\sqrt{b + cx}dx \quad \text{(B.3)}$$

Whereas, the integrals $J2$ and $J3$ can be written in the form

$$J2 = \int_0^\infty \exp(ax)\mathcal{K}_1\left(\sqrt{a_0 x + c_o}\right)\sqrt{b + cx}dx, \qquad \text{(B.4)}$$

and

$$J3 = \int_0^\infty \sqrt{x}\exp(ax)\mathcal{K}_1\left(\sqrt{a_0 x}\right)\mathcal{K}_1\left(\sqrt{a_0 x + c_o}\right)\sqrt{b + cx}dx, \qquad \text{(B.5)}$$

respectively, where, $a, b, c, a_0, b_0, c_0, d_0$ are constants. To the best of our knowledge, the integrals $J1, J2, J3$ and $J4$ cannot be solved in closed-form.

APPENDIX D

The expression for the non-zero secrecy rate is shown in (B.6) where $a_0 = 4\frac{i\lambda_{\mathrm{TR}}\lambda_{\mathrm{RD}}}{\gamma_M\xi}$, $b_0 = 4\frac{i\lambda_{\mathrm{TR}}\lambda_{\mathrm{RE}}}{\gamma_M\xi}$. $H_{C,D}^{A,B}[\cdot]$ is H function defined in [37, Eq. (1.1.1)]. (B.6) can be derived with the help of [38, Eq. (2.6)] and [37, Eq. (6.643.3)].

APPENDIX E

The expression for the ergodic secrecy rate is shown in (B.7) where $a_0 = 4\frac{i\lambda_{TR}\lambda_{RD}}{\gamma_M\xi}$, $b_0 = 4\frac{i\lambda_{TR}\lambda_{RE}}{\gamma_M\xi}$. (B.7) can be derived with the help of [38, Eq. (2.6)] and [37, Eq. (6.643.3)]. $J5$ can be written in the following form,

$$\int_0^\infty \frac{x}{1+x}\exp(ax)\mathcal{K}_1\left(\sqrt{a_0 x}\right)\mathcal{K}_1\left(\sqrt{b_0 x}\right)dx, \qquad \text{(B.8)}$$

where a, a_0, b_0 are constant. To the best of our knowledge, the integral $J5$ cannot be solved in closed-form.

REFERENCES

[1] O. Tipmongkolsilp, S. Zaghloul, and A. Jukan, "The evolution of cellular backhaul technologies: Current issues and future trends," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 1, pp. 97–113, 2011.

[2] X. Ge, H. Cheng, M. Guizani, and T. Han, "5G wireless backhaul networks: Challenges and research advances," *IEEE Netw.*, vol. 28, no. 6, pp. 6–11, Nov. 2014.

[3] K. J. Kim, P. L. Yeoh, P. V. Orlik, and H. V. Poor, "Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections," *IEEE Trans. Signal Process.*, vol. 64, no. 17, pp. 4403–4416, Sept. 2016.

[4] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[5] S. K. Satyanarayana, K. Sood, Y. Tao, and S. Yu, "Security and privacy in online social networks: A survey," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 1, no. 1, pp. 1–12, 2014.

[6] J. G. Andrews, "Seven ways that hetnets are a cellular paradigm shift," *IEEE Commun. Mag.*, vol. 51, no. 3, pp. 136–144, Mar. 2013.

[7] V. N. Q. Bao, T. Q. Duong, D. B. da Costa, G. C. Alexandropoulos, and A. Nallanathan, "Cognitive amplify-and-forward relaying with best relay selection in non-identical rayleigh fading," *IEEE Commun. Lett.*, vol. 17, no. 3, pp. 475–478, Mar. 2013.

[8] G. Chen, Z. Tian, Y. Gong, and J. Chambers, "Decode-and-forward buffer-aided relay selection in cognitive relay networks," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4723–4728, Nov. 2014.

[9] J. Yang, P. Fan, T. Q. Duong, and X. Lei, "Exact performance of two-way af relaying in nakagami-m fading environment," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 980–987, Mar. 2011.

[10] T. Q. Duong, L.-N. Hoang, and V. N. Q. Bao, "On the performance of two-way amplify-and-forward relay networks," *IEICE Trans. on Commun.*, vol. 92, no. 12, pp. 3957–3959, Dec. 2009.

[11] Y. Feng, S. Yan, Z. Yang, N. Yang, and W.-P. Zhu, "Tas-based incremental hybrid decode–amplify–forward relaying for physical layer security enhancement," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3876–3891, Jun. 2017.

[12] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 379–389, Feb. 2007.

[13] 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, Jul. 2013.

[14] Y. Feng, Z. Yang, W.-P. Zhu, Q. Li, and B. Lv, "Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2354–2366, Jun.

[15] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[16] T. Q. Duong, T. M. Hoang, C. Kundu, M. Elkashlan, and A. Nallanathan, "Optimal power allocation for multiuser secure communication in cooperative relaying networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 516–519, Oct. 2016.

[17] 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, May 2015.

[18] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Aug. 2016.

[19] Z. Shen, X. Zhang, M. Zhang, Z. Chen, W. Li, and H. Sun, "Information theory based performance analysis and enhancement of safety applications and cluster design in VANET," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 3, no. 6, pp. 1–10, 2016.

[20] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct. 2016.

[21] N.-P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, and L. Shu, "Secure 5g wireless communications: A joint relay selection and wireless power transfer approach," *IEEE Access*, vol. 4, pp. 3349–3359, Jun. 2016.

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2018.2794507, IEEE Access

$$
\begin{aligned}
\mathcal{P}_{out}(\theta) = {} & 1+\sum_{k=1}^{K}(-1)^k\binom{K}{k}s^k\exp\left(-\lambda_{TR}\frac{k(2^{2\theta}-1)}{\gamma_M}\right)\sum_{i=1}^{K}(-1)^i s^i\binom{K}{i}\\
& \sum_{i=1}^{K}(-1)^i s^i\binom{K}{i}2\frac{i\lambda_{TR}\lambda_{RE}}{\gamma_M\xi}\underbrace{\int_0^\infty\exp\left(-\lambda_{TR}\frac{k2^{2\theta}x}{\gamma_M}\right)\mathcal{K}_0\left(2\sqrt{\frac{\lambda_{TR}\lambda_{\mathsf{RE}}ix}{\gamma_M\xi}}\right)}_{J1}\\
& \underbrace{2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\right)dx}_{J1}\\
& -\sum_{k=1}^{K}(-1)^k\binom{K}{k}s^k\exp(-\lambda_{TR}\frac{k(2^{2\theta}-1)}{\gamma_M})\sum_{i=1}^{K}(-1)^i s^i\binom{K}{i}\frac{\lambda_{TE}s}{\gamma_M}\\
& \underbrace{\int_0^\infty\exp\left(-\lambda_{TR}\frac{k2^{2\theta}x}{\gamma_M}\right)2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right)}_{J2}\\
& \underbrace{\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\right)dx}_{J2}\\
& -2\sum_{k=1}^{K}(-1)^k\binom{K}{k}s^k\exp\left(-\lambda_{TR}\frac{k(2^{2\theta}-1)}{\gamma_M}\right)\sum_{i=1}^{K}(-1)^i s^i\binom{K}{i}s\sum_{j=1}^{K}(-1)^j s^j\binom{K}{j}2\sqrt{\frac{\lambda_{TR}\lambda_{RE}j}{\gamma_M\xi}}\frac{\lambda_{TE}}{\gamma_M}\\
& \underbrace{\int_0^\infty\exp\left(-\lambda_{TR}\frac{k2^{2\theta}x}{\gamma_M}\right)\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\right)}_{J3}\\
& \underbrace{\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RE}jx}{\gamma_M\xi}}\right)\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right)x^{\frac{1}{2}}dx}_{J3}\\
& -2\sum_{k=1}^{K}(-1)^k\binom{K}{k}s^k\exp(-\lambda_{TR}\frac{k(2^{2\theta}-1)}{\gamma_M})\sum_{i=1}^{K}(-1)^i s^i\binom{K}{i}s\sum_{k=1}^{K}(-1)^k s^k\binom{K}{k}\frac{2\lambda_{RE}k\lambda_{TR}}{\gamma_M\xi}\\
& \underbrace{\int_0^\infty\exp\left(-\lambda_{TR}\frac{k2^{2\theta}x}{\gamma_M}\right)\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i(2^{2\theta}-1)+\lambda_{TR}\lambda_{RD}i2^{2\theta}x}{\gamma_M\xi}}\right)}_{J4}\\
& \underbrace{\mathcal{K}_0\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RE}kx}{\gamma_M\xi}}\right)\exp\left(-\frac{\lambda_{TE}x}{\gamma_M}\right)dx}_{J4}
\end{aligned}
\tag{B.2}
$$

[22] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856–3867, Jun. 2016.

[23] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039–5051, Dec. 2015.

[24] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[25] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90–103, Jan. 2015.

[26] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sept. 2014.

[27] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.

[28] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, Jan. 2017.

[29] F. Shu, X. Wu, J. Li, R. Chen, and B. Vunetic, "Robust synthesis scheme for mult-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 5, pp. 6614–6623, Oct. 2016.

[30] J. Hu, F. Shu, and J. Li, "Robust synthesis method for secure directional modulation with imperfect angle information," *IEEE Commun. Lett.*, vol. 20, no. 16, pp. 1084–1087, Apr. 2016.

[31] T. A. Khan, P. Orlik, K. J. Kim, and R. W. Heath, "Performance analysis of cooperative wireless networks with unreliable backhaul links," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1386–1389, Aug. 2015.

[32] K. J. Kim, T. A. Khan, and P. V. Orlik, "Performance analysis of cooperative systems with unreliable backhauls and selection combining," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2448–2461, Mar. 2017.

[33] K. J. Kim, P. V. Orlik, and T. A. Khan, "Performance analysis of finite-sized co-operative systems with unreliable backhauls," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 5001–5015, Jul. 2016.

[34] H. T. Nguyen, J. Zhang, N. Yang, T. Q. Duong, and W.-J. Hwang,

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

$$\begin{aligned}
Pr(C_S > 0) = & \sum_{l=1}^{K}(-1)^l \binom{K}{l} s^l \sum_{m=1}^{K}(-1)^m s^m \binom{K}{m} \sqrt{\frac{\lambda_{TR}\lambda_{RD}i}{\gamma_M \xi}} \sum_{i=1}^{K}(-1)^i s^i \binom{K}{i} \frac{i\lambda_{TR}\lambda_{RE}}{\gamma_M \xi} \\
& (\frac{\lambda_{TR}l}{\gamma_M})^{-\frac{3}{2}} H^{1,0,0,2,2}_{1,(0,0),0,(2,2)} \left[\begin{array}{c|c} \frac{a_0 \gamma_M}{4\lambda_{TR}l} & (\frac{3}{2},1) \\ & - \\ \frac{b_0 \gamma_M}{4\lambda_{TR}l} & (\frac{1}{2},1);(\frac{1}{2},1);(0,0);(0,0) \end{array} \right] \\
& - \sum_{l=1}^{K}(-1)^l \binom{K}{l} \sum_{m=1}^{K}(-1)^m s^{m+l} \binom{K}{m} \frac{\lambda_{TE}s}{\gamma_M} 2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i}{\gamma_M \xi}} \frac{1}{\sqrt{a_0}} \exp\left(\frac{a_0\gamma_M}{8(\lambda_{TR}l + \lambda_{TE})}\right) \frac{\gamma_M}{\lambda_{TR}l + \lambda_{TE}} W_{-1,\frac{1}{2}}(\frac{a_0\gamma_M}{4(\lambda_{TR}l + \lambda_{TE})}) \\
& - \sum_{l=1}^{K}(-1)^l \binom{K}{l} \sum_{m=1}^{K}(-1)^m \binom{K}{m} \sqrt{\frac{\lambda_{TR}\lambda_{RD}m}{\gamma_M \xi}} \sum_{j=1}^{K}(-1)^j \binom{K}{j} \sqrt{\frac{\lambda_{TR}\lambda_{RE}j}{\gamma_M \xi}} \frac{\lambda_{TE}}{\gamma_M} s^{m+l+1+j} \\
& (\frac{\lambda_{TR}l + \lambda_{TE}}{\gamma_M})^{-2} H^{1,0,0,2,2}_{1,(0,0),0,(2,2)} \left[\begin{array}{c|c} \frac{a_0 \gamma_M}{4(\lambda_{TR}l + \lambda_{TE})} & (2,1) \\ & - \\ \frac{b_0 \gamma_M}{4(\lambda_{TR}l + \lambda_{TE})} & (\frac{1}{2},1);(\frac{1}{2},1);(\frac{1}{2},1);(\frac{1}{2},1) \end{array} \right] \\
& - \sum_{l=1}^{K}(-1)^l \binom{K}{l} \sum_{m=1}^{K}(-1)^m \binom{K}{m} \sqrt{\frac{\lambda_{TR}\lambda_{RD}i}{\gamma_M \xi}} \sum_{k=1}^{K}(-1)^k s^{m+l+k+1} \binom{K}{k} \frac{2\lambda_{RE}k\lambda_{TR}}{\gamma_M \xi} (\frac{\lambda_{TR}l + \lambda_{TE}}{\gamma_M})^{-\frac{2}{3}} \\
& H^{1,0,0,2,2}_{1,(0,0),0,(2,2)} \left[\begin{array}{c|c} \frac{a_0 \gamma_M}{4(\lambda_{TR}l + \lambda_{TE})} & (\frac{3}{2},1) \\ & - \\ \frac{b_0 \gamma_M}{4(\lambda_{TR}l + \lambda_{TE})} & (\frac{1}{2},1);(\frac{1}{2},1);(0,1);(0,1) \end{array} \right],
\end{aligned} \tag{B.6}$$

$$\begin{aligned}
\mathcal{C}_{erg} = & \frac{1}{4\ln(2)} \sum_{j=1}^{K}(-1)^j \binom{K}{j} s^j \sum_{l=1}^{K}(-1)^l s^l \binom{K}{l} 2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i}{\gamma_M \xi}} (\frac{\lambda_{TR}j}{\gamma_M})^{-2} H^{1,1,0,1,2}_{1,(1,0),0,(1,2)} \left[\begin{array}{c|c} \frac{\gamma_M}{\lambda_{TRj}} & (2,1) \\ & (0,1);- \\ & - \\ \frac{a_0\gamma_M}{4\lambda_{TR}j} & (0,1);(\frac{1}{2},1),(\frac{1}{2},1) \end{array} \right] \\
& + \frac{1}{2\ln(2)} \sum_{j=1}^{K}(-1)^j \binom{K}{j} s^j \sum_{l=1}^{K}(-1)^l s^l \binom{K}{l} \sqrt{\frac{\lambda_{TR}\lambda_{RD}i}{\gamma_M \xi}} \sum_{k=1}^{K}(-1)^k \binom{K}{k} s^k 4\sqrt{\frac{\lambda_{TR}\lambda_{RE}k}{\gamma_M \xi}} \\
& \underbrace{\int_0^\infty (\frac{1}{1+x}) \exp\left(-\lambda_{TR}\frac{jx}{\gamma_M}\right) \mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RD}ix}{\gamma_M \xi}}\right) x\mathcal{K}_1\left(2\sqrt{\frac{\lambda_{TR}\lambda_{RE}kx}{\gamma_M \xi}}\right) dx}_{J5} \\
& - \frac{1}{4\ln(2)} \sum_{j=1}^{K}(-1)^j \binom{K}{j} s^j \sum_{l=1}^{K}(-1)^l s^l \binom{K}{l} 2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i}{\gamma_M \xi}} s(\frac{\lambda_{\mathsf{TR}}j + \lambda_{TE}}{\gamma_M})^{-\frac{2}{3}} H^{1,1,0,1,2}_{1,(1,0),0,(1,2)} \left[\begin{array}{c|c} \frac{\gamma_M}{\lambda_{TRj} + \lambda_{\mathsf{TE}}} & (\frac{2}{3},1) \\ & (0,1);- \\ & - \\ \frac{a_0\gamma_M}{4(\lambda_{TR}j + \lambda_{TE})} & (0,1);(\frac{1}{2},1),(\frac{1}{2},1) \end{array} \right] \\
& - \frac{1}{4\ln(2)} \sum_{j=1}^{K}(-1)^j \binom{K}{j} s^j \sum_{l=1}^{K}(-1)^l s^l \binom{K}{l} 2\sqrt{\frac{\lambda_{TR}\lambda_{RD}i}{\gamma_M \xi}} s \sum_{i=1}^{K}(-1)^i \binom{K}{i} s^i 2\sqrt{\frac{\lambda_{TR}\lambda_{RE}i}{\gamma_M \xi}} \\
& (\frac{\lambda_{TR}j + \lambda_{TE}}{\gamma_M})^{-2} H^{1,1,0,1,2}_{1,(1,0),0,(1,2)} \left[\begin{array}{c|c} \frac{\gamma_M}{\lambda_{TRj} + \lambda_{TE}} & (2,1) \\ & (0,1);- \\ & - \\ \frac{a_0\gamma_M}{4(\lambda_{TR}j + \lambda_{TE})} & (0,1);(\frac{1}{2},1),(\frac{1}{2},1) \end{array} \right],
\end{aligned} \tag{B.7}$$

"Secure cooperative single carrier systems under unreliable backhaul and dense networks impact," *IEEE Access*, vol. 5, pp. 18 310–18 324, July 2017.

[35] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[36] N.-P. Nguyen, C. Kundu, H. Q. Ngo, T. Q. Duong, and B. Canberk, "Secure full-duplex small-cell networks in a spectrum sharing environment," *IEEE Access*, vol. 4, pp. 3087–3099, Jun. 2016.

[37] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. Academic press, 2007.

[38] A. M. Mathai and R. K. Saxena, "The h function with applications in statistics and other disciplines," 1978.

2169-3536 (c) 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.