Secure Cooperative Systems with Jamming and Unreliable Backhaul over Nakagami-m Fading Channels

Michael Stewart[1], Long D. Nguyen[1(✉)], Cheng Yin[1], Emiliano Garcia-Palacios[1], and Sang Q. Nguyen[2]

[1] School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, UK
{mstewart,lnguyen04,cyin}@qub.ac.uk, e.garcia@ee.qub.ac.uk
[2] Faculty of Information Technology, Duy Tan University, Da Nang, Vietnam
sangnqdv05@gmail.com

Abstract. In this paper, the secrecy performance of cooperative networks with jamming signals of eavesdroppers are studied under the impacts of unreliable backhaul networks. By proposing a two-phase transmitter/relay selection scheme, the desired signal-to-noise ratio (SNR) of relays is maximized by selected the best transmitter, meanwhile, the jamming signal-to-interference-plus-noise ratio (SINR) of the eavesdroppers is minimized by selected the best relay. The secrecy outage probability is derived in closed-form expressions by following some useful lemmas and theorems. Furthermore, the analysis of asymptotic secrecy outage probability is also performed to explicitly reveal the impacts of unreliable backhaul links on the secrecy performance. By the impact of imperfect backhaul links, the diversity gain is limited as shown in our results.

Keywords: Cooperative networks · Physical layer security
Secrecy performance · Unreliable backhaul

1 Introduction

Physical layer security (PLS) concept has become an emerging feature in wireless communication systems [14] with the serious effects of malicious eavesdroppers on the confidential transmission. In fact, the transmitted information might be vulnerable with the jamming interference by the existing of eavesdroppers [15] in

Supported by the Newton Prize 2017 and by a Research Environment Links grant, ID 339568416, under the Newton Programme Vietnam partnership. The grant is funded by the UK Department of Business, Energy and Industrial Strategy (BEIS) and delivered by the British Council. For further information, please visit www.newtonfund.ac.uk/.

T. Q. Duong and N.-S. Vo (Eds.): INISCOM 2018, LNICST 257, pp. 253–263, 2019.
https://doi.org/10.1007/978-3-030-05873-9_21

the wireless communication systems. For preventing eavesdropping attacks, the message between the source and destination is encrypted/decrypted with sharing the specific secretly key. To this end, PLS performs the information-theoretical methods, which involve the cooperative relaying to secure received messages at the receiver by exploiting the impact of jamming signals, to utilise the benefits of physical characteristics by different upper layer security [3]. On the other hand, cooperative networks (CNs) have grown in network infrastructure for satisfying the excessing increase of data transmission [8]. However, by deploying higher density of small-cell numbers, e.g., relay nodes, one of the critical problems of CNs is unreliable backhaul links [11,15,20]. Besides the threats of jamming interference from eavesdropping, the issues of propagation, e.g., multipath fading, transmission delay and synchronization can impact the reliable backhaul network as well as the network performance in CNs [13,16]. As a result, the unreliable backhaul transmissions significantly depreciate the performance of network [12,20].

Many previous PLS works ensure the success of the private signals from source to the legitimate destination under the assumption of ideal reliability backhaul link. In these studies, the cooperative relay technique is investigated to minimize the jamming interference of the eavesdroppers [4,9] under both decode-and-forward (DF) and amplify-and-forward (AF) relaying schemes [1,3,17]. However, in practice, the presence of unreliable backhaul cannot avoid since this issue strongly impacts the real network performance. Some researches have tackled the unreliable backhaul for enhancing the network performance [5,11,12,20]. For instances, the cooperative frameworks are proposed to scale the performance under the impact of unreliable backhaul links in [5,20] or the extension of spectrum sharing in backhaul communication with the limit interference of primary users [11,12].

From the observations of PLS and unreliable backhaul in CNs, it is obvious that the investigation of PLS under unreliable backhaul links has been completely necessary. In this paper, we study the network performance of a CN with the impact of jamming interference in term of secrecy outage probability. By exploiting a CN scenario, the unreliable backhaul links between a macro-cell and relay nodes (e.g., small-cells) is considered. This scheme is to eliminate the inter-symbol interference (ISI) [6,7]. On the other hand, the transmission information will be reflected by considering frequency selective fading channel [15,17]. Very recently, the performance of physical layer security has been investigated with single carrier system under the impact of imperfect backhaul condition [10]. To the best of our knowledge, all of the previous works on the physical layer security performance under the impact of unreliable backhaul only considered the Rayleigh fading channels. Therefore, in this paper, we take a step further to extend this research into a more general fading channel, namely, Nakagami-m. For the transmission scheme, a two-phase transmitter/relay selection scheme is provided in density multi-relay networks. The best relay selection is obtained in the first phase for maximizing the desired SNR at the relays and minimizing the signal-to-interference-plus-noise ratio (SINR) at the eavesdroppers during the second phase simultaneously. We show that the backhaul reliability is an important factor in PLS system design, which strongly affects the achievable secrecy performance.

Notation: $\mathcal{CN}(\mu, \sigma_n^2)$ denotes the complex Gaussian distribution with mean μ and variance σ_n^2; $\boldsymbol{I}_m$ is an $m \times m$ identity matrix; $\mathbb{C}^{m \times n}$ is vector space of $m \times n$ complex matrices; $X \sim \chi^2(N_X, \alpha_X)$ denotes chi-square distribution with degree of freedom (DoF) N_X and power normalizing constant α_X; $X \sim \text{Ga}(\mu_X, \eta_X)$ denotes Gamma distribution with shape μ_X and rate η_X. $F_\lambda(\gamma)$ and $f_\lambda(\gamma)$ denote the cumulative distribution function (CDF) and probability density function (PDF) of the random variable (RV) λ, respectively; $\mathbb{E}_\lambda\{f(\gamma)\}$ denotes the expectation of $f(\gamma)$ with respect to the RV λ. In addition, $\binom{\tau_1}{\tau_2} = \dfrac{\tau_1!}{\tau_2!(\tau_1 - \tau_2)}$ denotes the binomial coefficient.

2 Network and Channel Models

We consider a CN in where a macro-cell base station (Macro BS) connected to the core network as shown in Fig. 1. Meanwhile, K small-cell transmitters T_k, $k \in \{1, 2, \cdots, K\}$ connect to the Macro-BS via unreliable backhaul links and communicate with a destination (D) via M relays R_m, $m \in \{1, 2, \cdots, M\}$ applying DF scheme. Otherwise, a single jammer J and N eavesdroppers E_n, $n \in \{1, 2, \cdots, N\}$ exist in the network. Due to poor channel conditions, the direct link from T_k to destination and between T_k and E_n $\forall k \in K, \forall n \in N$ are neglected. On the other hand, the interference at the eavesdroppers is caused by J while the eavesdroppers cooperate to overhear the transmissions between R_m and D. In this work, we also assume that both of transmitters and receivers use half-duplex mode and exploit a single antenna.

For a cooperative system, we make the following assumptions for the channel model. Nakagami-m fading is considered in the channel model of the system. Therein, the channel between T_k and R_m, $\forall k, m$ is denoted by $h^{k,m} \sim \text{Ga}(\mu_k^m, \tilde{\eta}_k^m)$. Meanwhile, $g^{m,n} \sim \text{Ga}(\mu_m^n, \tilde{\eta}_m^n)$ denotes the channel between R_m and E_n, $\forall m, n$. The path loss component corresponding to $h^{k,m}$ and $g^{m,n}$ are denoted as $\alpha_T^{k,m}$ and $\alpha_E^{m,n}$, respectively. The channel between R_m and D, $\forall m$ and the channel between J and E_n, $\forall n$ are defined by $f^m \sim \text{Ga}(\mu_d^m, \tilde{\eta}_d^m)$ and $q^n \sim \text{Ga}(\mu_j^n, \tilde{\eta}_j^n)$. The path loss component corresponding to f^m and q^n are represented by α_D^m and α_J^n, respectively. We also assume that $\mathbb{E}[x] = \mathbb{E}[v] = 0$.

For all active links, the channel state information (CSI) is common assumed to be perfectly known at the relays, J, and D in PLS literature [3,15,18]. Also, the information can be measured by J from the eavesdroppers in the network [2]. The transmit symbol block $\boldsymbol{x}$, which is transmitted from the Macro-BS, must pass through the dedicated wireless backhaul links. The success/failure transmission represents the reception status at the K transmitters. Hence, a Bernoulli process $\mathbb{I}_k$ can be applied to the reliability of the wireless backhaul links, i.e., the message is successfully received at the receivers with a successful probability of λ_k. The failure probability is accordingly given by $1 - \lambda_k$ [5,12].

The received signal at R_m from T_k is expressed as

$$y_R^{k,m} = \sqrt{\mathcal{P}_t \alpha_T^{k,m}} h^{k,m} \mathbb{I}_k x + n_R^{k,m}, \tag{1}$$

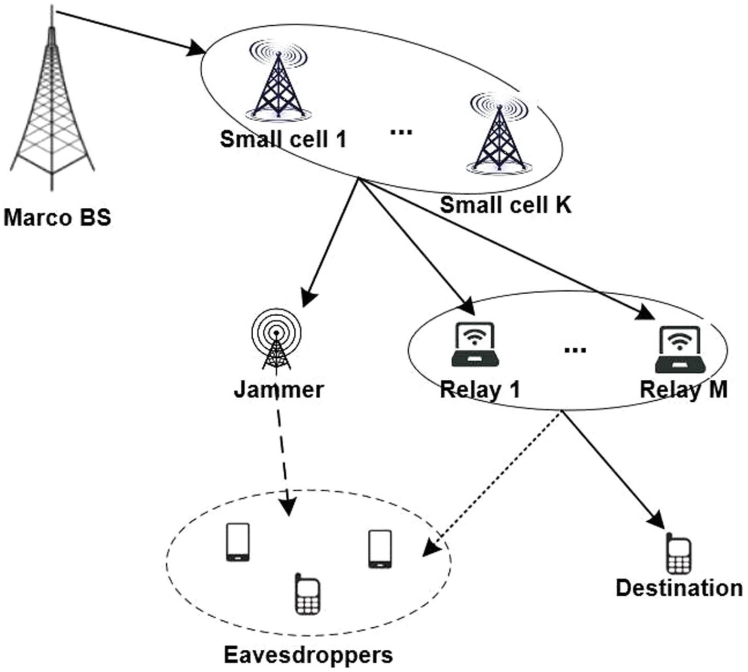

Fig. 1. System model.

where $\mathcal{P}_t$ is the transmit power and $n_R^{k,m} \sim \mathcal{CN}\left(0, \sigma_n^2\right)$ is an additive noise vector at R_m. $\mathbb{I}_k$ recalls the backhaul reliability which is modeled as a Bernoulli process. This model is common for the representation of the backhaul reliability with canonically success/failure transmission [5,12,15,20]. In the first time slot, the instantaneous SNR between T_k and R_m from (1) can be expressed as

$$\gamma_R^{k,m} = \frac{\mathcal{P}_t \alpha_T^{k,m} ||h^{k,m}||^2}{\sigma_n^2} \mathbb{I}_k = \widetilde{\alpha}_T^{k,m} ||h^{k,m}||^2 \mathbb{I}_k = \lambda^{k,m} \mathbb{I}_k, \tag{2}$$

where $\widetilde{\alpha}_T^{k,m} \triangleq \frac{\mathcal{P}_t \alpha_T^{k,m}}{\sigma_n^2}, \lambda^{k,m} \sim \mathrm{Ga}(\mu_k^m, \eta_k^m)$ with $\eta_k^m = \frac{\widetilde{\alpha}_T^{k,m} \, \mathbb{E}\left\{||h^{k,m}||^2\right\}}{\mu_k^m}$.

The received signals at E_n and D from R_m are given by

$$\begin{aligned} y_E^{m,n} &= \sqrt{\mathcal{P}_r \alpha_E^{m,n}} g^{m,n} x + \sqrt{\mathcal{P}_j \alpha_J^n} q^n v + n_E^{m,n}, \\ y_D^m &= \sqrt{\mathcal{P}_r \alpha_D^m} f^m x + n_D^m, \end{aligned} \tag{3}$$

where $\mathcal{P}_r$ and $\mathcal{P}_j$ are the transmit powers at the relays and J, respectively, $n_E^{m,n} \sim \mathcal{CN}(0, \sigma_n^2)$ and $n_D^m \sim \mathcal{CN}(0, \sigma_n^2)$ define the noise at E_n and D.

Therefore, the instantaneous SINR between R_m and E_n can be formulated as

$$\gamma_E^{m,n} = \frac{\mathcal{P}_r \alpha_E^{m,n} ||g^{m,n}||^2}{\sigma_n^2 + \mathcal{P}_j \alpha_J^n ||q^n||^2} = \frac{\widetilde{\alpha}_E^{m,n} ||g^{m,n}||^2}{1 + \widetilde{\alpha}_J^n ||q^n||^2} = \frac{\lambda^{m,n}}{1 + \lambda_J^n}, \tag{4}$$

where $\widetilde{\alpha}_E^{m,n} \triangleq \frac{\mathcal{P}_r \alpha_E^{m,n}}{\sigma_n^2}, \widetilde{\alpha}_J^n \triangleq \frac{\mathcal{P}_j \alpha_J^n}{\sigma_n^2}, \lambda^{m,n} \sim \mathrm{Ga}(\mu_m^n, \eta_m^n), \lambda_J^n \sim \mathrm{Ga}(\mu_j^n, \eta_j^n)$ with $\eta_m^n = \frac{\widetilde{\alpha}_E^{m,n} \mathbb{E}\left\{||g^{m,n}||^2\right\}}{\mu_m^n}, \eta_j^n = \frac{\widetilde{\alpha}_J^n \mathbb{E}\left\{||q^n||^2\right\}}{\mu_j^n}$.

In the remaining time slot, the instantaneous SNR between R_m and D can be expressed as

$$\gamma_D^m = \frac{\mathcal{P}_r \alpha_D^m ||f^m||^2}{\sigma_n^2} = \widetilde{\alpha}_D^m ||f^m||^2 = \lambda_D^m, \tag{5}$$

where $\widetilde{\alpha}_D^m \triangleq \frac{\mathcal{P}_r \alpha_D^m}{\sigma_n^2}, \lambda_D^m \sim \mathrm{Ga}(\mu_d^m, \eta_d^m)$ with $\eta_d^m = \frac{\widetilde{\alpha}_D^m \mathbb{E}\left\{||f^m||^2\right\}}{\mu_d^m}$.

Moreover, the channels are distributed according to chi-square distribution since they are assumed to undergo Nakagami-m fading. Thus, the CDF and PDF of RV $\chi \sim \mathrm{Ga}(\mu_\chi, \eta_\chi)$, where $\chi \in \{h^{k,m}, g^{m,n}, f^m, q^n\}$ are given, respectively,

$$f_\chi(x) = \frac{1}{(\mu_\chi - 1)!(\eta_\chi)^{\mu_\chi}} x^{\mu_\chi - 1} e^{(-x/\eta_\chi)},$$

$$F_\chi(x) = 1 - e^{(-x/\eta_\chi)} \sum_{i=0}^{\mu_\chi - 1} \frac{1}{i!} \left(x/\eta_\chi\right)^i, \tag{6}$$

respectively. We assume that the unreliable backhaul links are independent from the indices of the K transmitters, i.e., $\lambda_k = \lambda, \forall k$ and the positive fading severity parameter μ_χ and η_χ are identically varied among the K transmitters, M relays and N eavesdroppers, i.e., $\mu_T = \mu_k^m, \mu_E = \mu_m^n, \mu_J = \mu_j^n, \mu_D = \mu_d^m$, and $\eta_T = \eta_k^m, \eta_E = \eta_m^n, \eta_J = \eta_j^n, \eta_D = \eta_d^m, \forall k, m, n$.

3 Secrecy Performance Analysis

3.1 Two-Phase Transmitter/Relay Selection Scheme

By providing a two-phase selection scheme, our target is to achieve high PLS level. This scheme is to maximizes the achievable performance and minimizes the undesired performance at the eavesdroppers simultaneously. Following this intuition, in the first phase, each relay chooses the best transmitter among the K small-cells to maximize their achievable SNR. The selected scheme in the first phase can be mathematically expressed as

$$\text{Phase 1:} \quad k^* = \arg \max_{k=1,\ldots,K} \gamma_R^{k,m}, \tag{7}$$

where $\gamma_R^{k,m}$ recalls the instantaneous SNR at R_m via T_k. From (7), the statistical property of the instantaneous SNR via the best transmitter T_{k^*} is given in the following theorem.

Theorem 1. *Given K independent and identical unreliable backhaul connections, the CDF of the received SNR at R_m via the best transmitter is given as*

$$F_{\gamma_R^{k^*,m}}(x) = 1 + \sum_{k=1}^{K} \sum_{\omega_1,\ldots,\omega_{\mu_R}}^{k} \binom{K}{k} \left(\frac{k!}{\omega_1!\ldots\omega_{\mu_R}!}\right) \frac{(-1)^k \lambda^k}{\prod_{t=0}^{\mu_R-1} (t!(\eta_T)^t)^{\omega_{t+1}}} x^{\sum_{t=0}^{\mu_R-1} t\omega_{t+1}} e^{-kx/\eta_T}. \quad (8)$$

Proof. The proof will show in the journal version by the limit of conference version.

The relay selection will be implemented in the second phase, which is to minimize the SINR between the particular relay and N eavesdroppers. This scheme can be formulated as

$$\text{Phase 2:} \quad m^* = \arg \min_{m=1,\ldots,M} \gamma_E^{m,n^*} \quad , \quad (9)$$

where $\gamma_E^{m,n^*} = \max(\gamma_E^{m,1}, ..., \gamma_E^{m,N})$ is the maximum instantaneous SINR between R_m and N eavesdroppers. The CDF of the RV γ_E^{m,n^*} is given in the following lemma and theorems in [10].

3.2 Secrecy Outage Probability

In this subsection, we focus on the secrecy outage probability, where the eavesdroppers's CSI is assumed unavailable in the considered network. In this case, the transmitters encode and send the confidential message with the constant secrecy rate of θ. If the instantaneous secrecy capacity, denoted by $\mathcal{C}_S$ in bits/s/Hz, is greater than θ, the secrecy gain is guaranteed. To study the asymptotic behavior, the asymptotic secrecy outage probability will be analysed in this work.

Following [19], the secrecy capacity $\mathcal{C}_S$ can be expressed as

$$\mathcal{C}_S = \frac{1}{2}\left[\log_2(1+\widetilde{\gamma}_{DF}^{m^*}) - \log_2(1+\gamma_E^{m^*,n^*})\right]^+, \quad (10)$$

where $\log_2(1+\widetilde{\gamma}_{DF}^{m^*})$ is the instantaneous capacity at D respect to the m^*-th relay and $\log_2(1+\gamma_E^{m^*,n^*})$ is the instantaneous capacity of the m^*-th relay and n^*-th eavesdropper link.

Thus, the secrecy outage probability, i.e. the probability when the secrecy capacity (10) falls below the given rate threshold, can be expressed as [17]

$$\begin{aligned}\mathcal{P}_{out}(\theta) &= Pr(\mathcal{C}_S < \theta) \\ &= \int_0^\infty F_{\widetilde{\gamma}_{DF}^{m^*}}\left(2^{2\theta}(1+x)-1\right) f_{\gamma_E^{m^*,n^*}}(x)\, dx. \end{aligned} \quad (11)$$

$$\mathcal{P}_{out}(\theta) = 1 + \mathcal{Q}\widetilde{\sum_{D}}\widetilde{\sum_{E}}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}(\Upsilon-1)^{\beta-\alpha}(\Upsilon)^{\alpha}\eta_E^{\widetilde{\varphi}_3}e^{-\Phi(\Upsilon-1)}(\mathcal{O}_1-\mathcal{O}_2+\mathcal{O}_3), \quad (12)$$

where $\Upsilon \triangleq 2^{2\theta}$, $\epsilon \triangleq \frac{\eta_E}{\eta_J}$ and

$$\mathcal{O}_1 = \mathcal{B}_1\Gamma(\widetilde{\varphi}_2+\alpha+1)\epsilon^{\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+1, \widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3, \epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)\right),$$
$$\mathcal{O}_2 = \mathcal{B}_2\Gamma(\widetilde{\varphi}_2+\alpha)\epsilon^{\widetilde{\varphi}_2+\alpha-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha, \widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3, \epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)\right),$$
$$\mathcal{O}_3 = \mathcal{B}_3\Gamma(\widetilde{\varphi}_2+\alpha+2)\epsilon^{\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+2, \widetilde{\varphi}_2+\alpha+3-\widetilde{\varphi}_3, \epsilon(\Phi\Upsilon+\widetilde{\varphi}_1)\right).$$

$$\mathcal{P}_{out}^{\infty}(\theta) \overset{\eta_D\to\infty}{=} 1 + \mathcal{Q}\widetilde{\sum_{D^\infty}}\widetilde{\sum_{E}}\sum_{\alpha=0}^{\tilde{\beta}}\binom{\tilde{\beta}}{\alpha}(\Upsilon-1)^{\tilde{\beta}-\alpha}(\Upsilon)^{\alpha}\eta_E^{\widetilde{\varphi}_3}e^{-\tilde{\Phi}(\Upsilon-1)}(\widehat{\mathcal{O}_1}-\widehat{\mathcal{O}_2}+\widehat{\mathcal{O}_3}), \quad (13)$$

where $\tilde{\beta} = \sum_{t=0}^{\mu_R-1} t\omega_{t+1}$, $\tilde{\Phi} = \frac{k}{\eta_T}$, $\widetilde{\sum_{D^\infty}} = \sum_{k=1}^{K}\sum_{\omega_1,\ldots,\omega_{\mu_R}}^{k}\binom{K}{k}\left(\frac{k!}{\omega_1!\ldots\omega_{\mu_R}!}\right)\frac{(-1)^{k-1}\lambda^k}{\prod_{t=0}^{\mu_R-1}(t!(\eta_T)^t)^{\omega_{t+1}}}$, and

$$\widehat{\mathcal{O}_1} = \mathcal{B}_1\Gamma(\widetilde{\varphi}_2+\alpha+1)\epsilon^{\widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+1, \widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right),$$
$$\widehat{\mathcal{O}_2} = \mathcal{B}_2\Gamma(\widetilde{\varphi}_2+\alpha)\epsilon^{\widetilde{\varphi}_2+\alpha-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha, \widetilde{\varphi}_2+\alpha+1-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right),$$
$$\widehat{\mathcal{O}_3} = \mathcal{B}_3\Gamma(\widetilde{\varphi}_2+\alpha+2)\epsilon^{\widetilde{\varphi}_2+\alpha+2-\widetilde{\varphi}_3}\Psi\left(\widetilde{\varphi}_2+\alpha+2, \widetilde{\varphi}_2+\alpha+3-\widetilde{\varphi}_3, \epsilon(\tilde{\Phi}\Upsilon+\widetilde{\varphi}_1)\right).$$

The closed-from expression for the secrecy outage probability in (11) is given in the following theorem.

Theorem 2. *For the CN with unreliable backhaul links, the secrecy outage probability with two-phase transmitter/relay selection scheme is given as in (12) at the top of next page.*

Proof. The proof will be provided in the journal version by the limit of conference version.

To study the impacts of unreliable backhaul connections, the asymptotic expression for the secrecy outage probability is given in the following theorem.

Theorem 3. *Given the fixed set $\{\eta_T, \eta_E, \eta_J\}$, the asymptotic expression for secrecy outage probability is given as (13) at the top of next page.*

Proof. The proof will be provided in the journal version by the limit of conference version.

From (13), due to the unreliable backhaul links, the secrecy diversity gain is not achievable. Furthermore, the limitation on secrecy outage probability is determined as a constant since the asymptotic secrecy outage is independent of DoF of channels between relay and D.

4 Numerical Results

In this section, we validate our analysis and investigate the secrecy outage probability of the considered system model by providing the numerical results. In our simulation, we deploy the binary phase-shift keying (BPSK) modulation with transmission block size $S = 64$ symbols. For convenience, we define Ex and An as the results of link-level simulations and the analytical results, respectively. In the following, we investigate the network performance with various parameters to examine the effects of the degrees of cooperative transmission, DoFs, and backhaul reliability.

4.1 Secrecy Outage Probability

Fig. 2 illustrates the secrecy outage probability for various M and N. The network parameters are set as $K = 3, \lambda = 0.995, \{\mu_R, \mu_E, \mu_J, \mu_D\} = \{2, 2, 2, 3\}$, and $\{\eta_T, \eta_E, \eta_J\} = \{10, 10, 10\}$ dB. It can be observed that the number of relays/eavesdroppers strongly affects the secrecy outage probability. For example, when $N = 1$, the secrecy outage probability becomes lower when more relays help with the cooperative transmission. Differently, when $M = 1$, the secrecy outage probability becomes higher when the number of eavesdroppers increases. This is due to the fact that when the number of relays increases, the secrecy rate becomes higher as a result of the reduction in the wiretap channel capacity. Similarly, the secrecy rate decreases proportionally to the increase in the number of eavesdroppers. We further see that our analysis precisely matches the simulations and our analysis approaches the asymptotic results, presented in Theorem 3, in the high SNR regime.

In Fig. 3, we investigate the effects of DoFs and $\{\eta_T, \eta_E, \eta_J\}$ on the secrecy outage probability. In the settings, we set $K = 3, M = 1, N = 2, \lambda = 0.98$, and $\{\mu_R, \mu_E, \mu_J\} = \{2, 2, 4\}$. As μ_D increases, we observe that the lower secrecy outage probability is achieved. We also observe that as η_T and η_J increase, the secrecy outage probability becomes lower while the increase in η_E results in high achievable secrecy outage. It is clearly to see that the increase in η_T results in a high received power at the receiver while the increase in η_J reduces the SINR of the eavesdroppers.

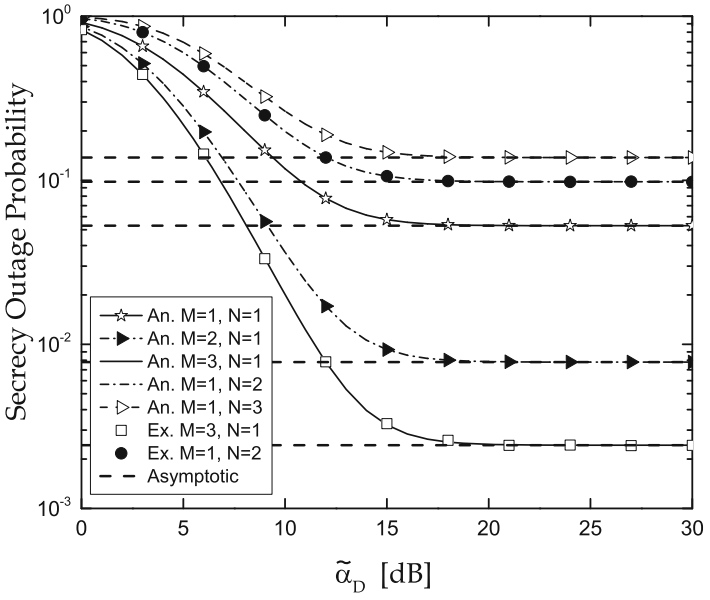

Fig. 2. Secrecy outage probability for various M, N of the proposed network.

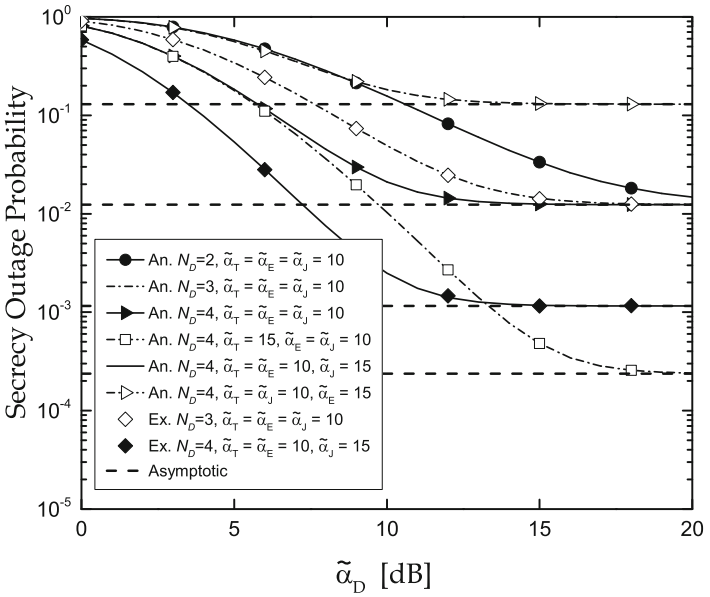

Fig. 3. Secrecy outage probability for various DoFs and $\{\eta_T, \eta_E, \eta_J\}$ of the proposed network.

5 Conclusions

This work has studied the impacts of unreliable backhaul links on the secrecy performance of a CN. A two-phase transmitter/relay selection scheme was proposed to minimize the information overheard of the eavesdroppers with guaranteeing the requirement of the instantaneous SNR at the receiver. The secrecy outage probability is analysed and derived to the exact expressions. For high SNRs regime, the asymptotic expressions of secrecy outage probability were attained to investigate the network performance. The simulation results demonstrated that the impact of backhaul reliability is an important parameter for the improvement of the secrecy performance.

Acknowledgement. This work was supported by the Newton Prize 2017 and by a Research Environment Links grant, ID 339568416, under the Newton Programme Vietnam partnership. The grant is funded by the UK Department of Business, Energy and Industrial Strategy (BEIS) and delivered by the British Council. For further information, please visit www.newtonfund.ac.uk/

References

1. Bao, V.N.Q., Linh-Trung, N., Debbah, M.: Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. IEEE Trans. Wirel. Commun. **12**(12), 6076–6085 (2013)
2. Bloch, M., Barros, J., Rodrigues, M.R., McLaughlin, S.W.: Wireless information-theoretic security. IEEE Trans. Inf. Forensics Secur. **54**(6), 2515–2534 (2008)
3. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
4. Hoang, T.M., Duong, T.Q., Vo, N.S., Kundu, C.: Physical layer security in cooperative energy harvesting networks with a friendly jammer. IEEE Wirel. Commun. Lett. **6**(2), 174–177 (2017)
5. Khan, T.A., Orlik, P., Kim, K.J., Heath, R.W.: Performance analysis of cooperative wireless networks with unreliable backhaul links. IEEE Commun. Lett. **19**(8), 1386–1389 (2015)
6. Kim, K.J., Duong, T.Q., Elkashlan, M., Yeoh, P.L., Poor, H.V., Lee, M.H.: Spectrum sharing single-carrier in the presence of multiple licensed receivers. IEEE Trans. Wirel. Commun. **12**(10), 5223–5235 (2013)
7. Kim, K.J., Duong, T.Q., Tran, X.N.: Performance analysis of cognitive spectrum-sharing single-carrier systems with relay selection. IEEE Trans. Signal Process. **60**(12), 6435–6449 (2012)
8. Krikidis, I., Thompson, J.S., Mclaughlin, S.: Relay selection for secure cooperative networks with jamming. IEEE Trans. Wirel. Commun. **8**(10), 5003–5011 (2009)
9. Liu, W., Zhou, X., Durrani, S., Popovski, P.: Secure communication with a wireless-powered friendly jammer. IEEE Trans. Wirel. Commun. **15**(1), 401–415 (2016)
10. Nguyen, H.T., Zhang, J., Yang, N., Duong, T.Q., Hwang, W.J.: Secure cooperative single carrier systems under unreliable backhaul and dense networks impact. IEEE Access **5**, 18310–18324 (2017)

11. Nguyen, H.T., Duong, T.Q., Hwang, W.J.: Multiuser relay networks over unreliable backhaul links under spectrum sharing environment. IEEE Commun. Lett. **21**, 1–4 (2017). Accepted and appeared on IEEE Xplorer
12. Nguyen, H.T., Ha, D.B., Nguyen, S.Q., Hwang, W.J.: Cognitive heterogeneous networks with unreliable backhaul connections. J. Mobile Netw. Appl. (MONET) (2017)
13. Pantisano, F., Bennis, M., Saad, W., Debbah, M., Latva-Aho, M.: On the impact of heterogeneous backhauls on coordinated multipoint transmission in femtocell networks. In: Proceedings of IEEE International Conference on Communications, Ottawa, Canada, pp. 5064–5069, June 2012
14. Rodriguez, L.J., Tran, N.H., Duong, T.Q., Le-Ngoc, T., Elkashlan, M., Shetty, S.: Physical layer security in wireless cooperative relay networks: state of the art and beyond. IEEE Commun. Mag. **53**(12), 32–39 (2015)
15. Shafie, A.E., Duong, T.Q., Al-Dhahir, N.: QoS-aware enhanced-security for TDMA transmissions from buffered source nodes. IEEE Trans. Wirel. Commun. **16**(2), 1051–1065 (2017)
16. Simeone, O., Somekh, O., Erkip, E., Poor, H.V., Shitz, S.S.: Robust communication via decentralized processing with unreliable backhaul links. IEEE Trans. Inf. Theory **57**(7), 4187–4201 (2011)
17. Wang, L., Kim, K.J., Duong, T.Q., Elkashlan, M., Poor, H.V.: Security enhancement of cooperative single carrier systems. IEEE Trans. Inf. Forensics Secur. **10**(1), 90–103 (2015)
18. Yang, J., Kim, I.M., Kim, D.I.: Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers. IEEE Trans. Wirel. Commun. **12**(6), 2840–2852 (2013)
19. Yang, N., Suraweera, H.A., Collings, I.B., Yuen, C.: Physical layer security of TAS/MRC with antenna correlation. IEEE Trans. Inf. Forensics Secur. **8**(1), 254–259 (2013)
20. Yin, C., Nguyen, H.T., Kundu, C., Kaleem, Z., Garcia-Palacios, E., Duong, T.Q.: Secure energy harvesting relay networks with unreliable backhaul connections. IEEE Access **6**, 12074–12084 (2018)