Secrecy Performance of Small-Cell Networks over Nakagami-m Fading in the Presence of Unreliable Backhaul and Imperfect CSI

Cheng Yin*, Trung Q. Duong†, and Pei Xiao*
* University of Surrey, UK, email: {c.yin, p.xiao}@surrey.ac.uk
† Queen's University Belfast, UK, email: trung.q.duong@qub.ac.uk

***Abstract*—This paper investigates the impact of unreliable backhaul and channel estimation error on the performance of small-cell networks over independent and identically distributed Nakagami-m fading channels. To overcome the impact of these practical constraints, we propose an optimal selection scheme where the best small cell with respect to the maximal secrecy capacity is selected. The secrecy outage probability for the considered scheme is derived and compared with Monte-Carlo simulations. To gain additional insights on the impact of unreliable backhaul and imperfect channel estimation, the asymptotic behaviour of secrecy outage probability is also obtained.**

I. Introduction

Traditionally, telecommunication networks have relied on backhaul to convey traffic from the access to the core network. A variety of physical media has been used, such as copper, optical fibre and radio. The latter constitutes the so-called wireless backhaul [1]. Although there is a clear advantage to the huge capacity provided by the fibre wired backhaul, the lack of ubiquitous fibre availability and the expense to deploy such fibre soon made a case for a wireless backhaul alternative. Heterogeneous networks provide effective means of accommodating the current growth of data traffic by deploying macro base stations with a large number of small-cells (i.e., microcells, picocells and femtocells) and access points, thus expanding the coverage and offloading the traffic. Wireless backhaul is proved as an effective way to provide communication links for the small-cells and access points in outdoor scenarios where wired links are unavailable, even though it suffers from unreliability [2].

Due to the requirement for ultra-connectivity in heterogeneous networks, a large number of devices bring threats to wireless security, and the wireless uncertainties even make them more vulnerable to attack [3]. Hence, secure heterogeneous networks in the presence of wireless backhaul unreliability have been regarded as an attractive research topic. Pysical layer security (PLS) which has been largely investigated due to the ability to guarantee secrecy and combat eavesdroppers even without encryption [4]. The principle of PLS is to ensure reliable communications by exploiting random and unpredictable features of wireless channels [5]. In heterogeneous networks, the small-cell transmitter selection approach is the most simple and desirable way to achieve diversity gains for low-complexity terminals [6]. Only channel state information (CSI) feedback is needed during the selection procedure without requiring extra resources.

Existing research [7], [8] has studied the impact of wireless backhaul on secrecy performance in PLS networks. To enhance the secrecy performance with unreliable backhaul, a friendly jammer and cooperative relays were considered in a secure single carrier system [7]. Transmitter selection approaches have been utilized in performance analysis under wireless backhaul uncertainties [8]. The above literature revealed that backhaul reliability imposes limitations on the system secrecy performance and should be considered in the system performance analysis. However, it is important to note that these studies assume perfect knowledge of CSI at destinations. In practical wireless networks, this assumption of perfect CSI is not realistic. Therefore, it is imperative to consider how this inaccurate channel knowledge affects the system secrecy performance with wireless backhaul uncertainties.

More importantly, related research [6], [8] examined the impact of wireless backhaul on system performance in PLS networks. However, [8] assumed that channel estimation is perfect and [6] assumed that the legitimate and wiretap links follow Rayleigh fading, which is only a special case of Nakagami-m fading. The two assumptions are not generic and practical in real scenarios. In this work, we consider imperfect CSI at the destinations in the proposed system. We assume that transmission links follow Nakagami-m fading channel, which is regarded as the most generalized model of different fading channels. For instance, Rayleigh fading channel and Rician fading channel can be modelled by adjusting the value of m [9]. In addition, we propose a novel Optimal small-cell transmitter Selection (OS) scheme to improve the secrecy performance under wireless backhaul uncertainties and channel estimation errors.

II. System Model

We investigate a secure network where a macro base station, BS, connects to K small-cell transmitters, T_k, $\forall$ $k \in \{1, \cdots, K\}$, through unreliable wireless backhaul. The best small-cell transmitter T_{k^*} is chosen for transmission to the destination D while an eavesdropper E is wiretapping, as shown in Fig.1. The point-to-point microwave links, especially operated at higher frequencies, behave as success in ideal scenarios and failure when there are severe fading [2]. Therefore, we model the backhaul reliability as a Bernoulli process $\mathbb{I}_k$, which has been used in recent research [10]. The success probability of wireless backhaul is assumed as p_k and

978-1-6654-6975-3/22/$31.00 ©2022 IEEE

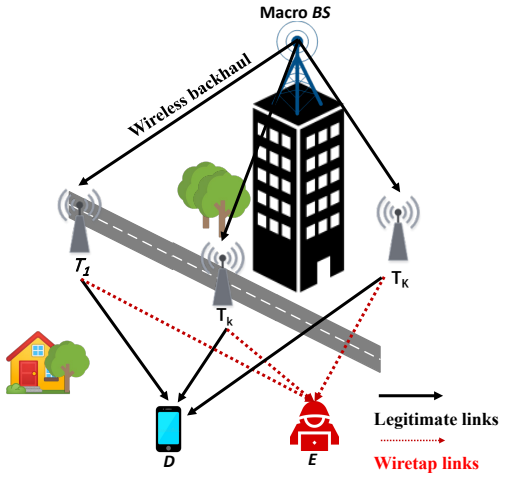

Fig. 1. A secure heterogeneous network with wireless backhaul and imperfect channel estimation

the failure probability is $1-p_k$, where $\mathbb{P}(\mathbb{I}_k=1)=p_k$ and $\mathbb{P}(\mathbb{I}_k=0)=1-p_k$. Due to the practical limitation of acquiring CSI, we assume that the channel estimation at E and D is imperfect.

We assume that all channels, including the main channel from T_k to D and wiretap channel from T_k to E, follow independent and identically distributed (i.i.d) Nakagami-m fading [11]. The assumption of applying i.i.d fading channels has been made in relevant research in heterogeneous network [6]. This system model can also be extended over independent but non-identically distributed (i.n.i.d) fading channels with similar methods.

The channel power gains $|h_X|^2$ undergo the gamma distribution with mean power Ω_X, and fading parameter m_X, where $X \in \{T_kD, T_kE\}$. The Cumulative Distribution Function (CDF) of X, denoted as $F_X(\cdot)$, and Probability Distribution Function (PDF) of X, denoted as $f_X(\cdot)$, can be written as:

$$\begin{aligned} F_X(x) &= 1-\exp\left(-\frac{x}{\theta_X}\right)\sum_{i=0}^{m_X-1}\frac{1}{i!}\left(\frac{x}{\theta_X}\right)^i, \\ f_X(x) &= \frac{x^{m_X-1}}{\Gamma(m_X)\theta_X^{m_X}}\exp\left(-\frac{x}{\theta_X}\right), \end{aligned} \tag{1}$$

where $\theta_X=\frac{\Omega_X}{m_X}$, and $\Gamma(\cdot,\cdot)$ represents the incomplete gamma function [12, (8.352.6)].

During the transmission, D and E receive the signals from T_k, and T_k which connect to macro BS via wireless backhaul. Therefore, the received signals at D and E are given as:

$$\begin{aligned} y_D &= \sqrt{P_T}h_{T_kD}\mathbb{I}_k x+z, \\ y_E &= \sqrt{P_T}h_{T_kE}x+z, \end{aligned} \tag{2}$$

where h_{T_kD} and h_{T_kE} denote the channel coefficients from T_k to D and from T_k to E. In addition, x is the unit power transmitted symbol and P_T is assumed to be the transmit power. The noises of D and E are complex additive white Gaussian noise (AWGN) with zero mean and variance σ, i.e., $z\sim CN(0,\sigma^2)$, and represented as z. It is to be noted that, only the received signal at D experiences the backhaul reliability $\mathbb{I}_k$. This is because E can intercept the transmission only when T_k is transmitting. Otherwise, E cannot wiretap if the legitimate transmission fails.

In practical communication systems, CSI cannot be perfectly estimated at D and E. Therefore, the mathematical expression of estimated channel coefficients $\widehat{h}_{T_kD}$, $\widehat{h}_{T_kE}$ and real channel coefficients h_{T_kD}, h_{T_kE} are expressed as

$$\begin{aligned} h_{T_kD} &= \widehat{h}_{T_kD}+e_{TD}, \\ h_{T_kE} &= \widehat{h}_{T_kE}+e_{TE}, \end{aligned} \tag{3}$$

where e_{TD} and e_{TE} are the estimation errors, i.e., $e_{TD}\sim CN(0,\epsilon_D^2)$, $e_{TE}\sim CN(0,\epsilon_E^2)$. With regard to the rule of channel estimation, $\epsilon_D^2=E[|h_{T_kD}|^2]-E[|\widehat{h}_{T_kD}|^2]$, under the assumption that $\widehat{h}_{T_kD}$ and e_{TD} are statistically independent. This is the same for the eavesdropping channel. For simplicity, we assume that e_{TD} and e_{TE} undergo the same distribution, $CN(0,\epsilon^2)$, where $\epsilon_D^2=\epsilon_E^2=\epsilon^2$. Due to the practical constraints of channel estimation, the estimated channel coefficients can be regarded as the real coefficients distorted with an extra error. Imperfections are due to, for example, noises and hardware impairments [13].

After investigating the imperfect channel estimation errors, we apply (3) into (2), then the received signals with both uncertainties of backhaul and channel estimation can be rewritten as:

$$\begin{aligned} y_D &= \sqrt{P_T}(\widehat{h}_{T_kD}+e_{TD})\mathbb{I}_k x+z, \\ y_E &= \sqrt{P_T}(\widehat{h}_{T_kE}+e_{TE})x+z. \end{aligned} \tag{4}$$

Based on (4), the instantaneous SNRs at D and E are provided as,

$$\begin{aligned} SNR_{TD} &= \frac{P_0|h_{T_kD}|^2\mathbb{I}_k}{P_0\epsilon^2\mathbb{I}_k+1}, \\ SNR_{TE} &= \frac{P_0|h_{T_kE}|^2}{P_0\epsilon^2+1}, \end{aligned} \tag{5}$$

where $P_0=\frac{P_T}{\sigma^2}$.

According to the instantaneous SNRs at D and E, the overall secrecy capacity can be written as:

$$C=[\log_2(1+SNR_{TD})-\log_2(1+SNR_{TE})]^+. \tag{6}$$

where $[x]^+$ denotes $\max(x,0)$. Then we perform OS scheme to select the best transmitter T_{k^*} by searching the T_k that can achieve maximum overall secrecy capacity. The OS scheme aims to achieve the highest overall secrecy capacity C, which can be defined as:

$$k^*=\arg\max\left[\log_2(1+SNR_{k^*D})-\log_2(1+SNR_{k^*E})\right]^+, \tag{7}$$

where k^* refers to the index of the selected transmitter and $SNR_{T_{k^*}D}$ and $SNR_{T_{k^*}E}$ are presented as:

$$SNR_{T_{k^*}D} = \frac{P_0|h_{T_{k^*}D}|^2\mathbb{I}_{k^*}}{P_0\epsilon^2\mathbb{I}_{k^*}+1}, \\ SNR_{T_{k^*}E} = \frac{P_0|h_{T_k^*E}|^2}{P_0\epsilon^2+1}, \tag{8}$$

where $|h_{T_{k^*}D}|^2$ and $|h_{T_k^*E}|^2$ represent the channel coefficients of T_{k^*} to D and E. $\mathbb{I}_{k^*}$ represents the backhaul reliability from macro BS to T_{k^*}.

Note that this novel OS scheme is proposed to enhance secrecy performance under the practical constraints of wireless backhaul imperfections and channel estimation errors.

III. Secrecy Performance analysis

We use Secrecy Outage Probability (SOP) to evaluate the system secrecy performance. SOP is one of the well-known performance metrics in PLS and is defined as the probability that the overall secrecy capacity C is below a certain threshold R_{th}. Our main contribution is to generalize the parameters of uncertainties from wireless backhaul and channel estimation into performance analysis in terms of SOP.

The definition of SOP is expressed as [14]:

$$\mathbb{P}_{\text{out}}(\theta) = \mathbb{P}_{\text{out}}(C_s < \theta) \\ = \int_0^\infty F_{TD}(\rho(1+x)-1)f_E(x)dx. \tag{9}$$

where $\rho = 2^{R_{th}}$.

Then we generalize the wireless backhaul reliability $\mathbb{I}_k$ into the PDF and CDF of random variable X. The CDF and PDF of random variable $\mathbb{I}_k X$ over i.i.d Nakagami-m fading channels can be further extended to:

$$F_{\mathbb{I}_k X}(x) = 1 - p\exp\left(-\frac{x}{\theta_X}\right)\sum_{i=0}^{m_X-1}\frac{1}{i!}\left(\frac{x}{\theta_X}\right)^i, \\ f_{\mathbb{I}_k X}(x) = p\frac{x^{m_X-1}}{\Gamma(m_X)\theta_X^{m_X}}\exp\left(-\frac{x}{\theta_X}\right) + (1-p)\delta(x). \tag{10}$$

We assume that p_k is identical for each link, as p_k=p, $\forall k$. This can be extended to non-identical cases for further study using the same method. In this work, we focus on the impact of this uncertainty on secrecy performance, therefore we assume that p_k is identical for simplicity.

With the help of (10), we could derive the SOP of the overall system as follows:

$$\mathbb{P}_{\text{out}}^{OS} = 1 + \sum_{k=1}^{K}\binom{K}{k}(-1)^k p^k \exp\left(-\frac{k(P_0\epsilon^2 p+1)(\rho-1)}{P_0\theta_D}\right) \\ \sum_{w_1+w_2+\ldots+w_{m_D}=k}\binom{k!}{w_1!w_2!\ldots w_{m_D}!}\left(\frac{\rho-1}{\rho}\right)^{m_E k} \\ \frac{(\rho-1)^{\sum_{t=0}^{m_D-1}tw_{t+1}}}{\prod_{t=0}^{m_D-1}\left(t!\left(\frac{P_0\theta_D}{P_0\epsilon^2 p+1}\right)^t\right)^{w_{t+1}}}\left(\frac{P_0\epsilon^2+1}{P_0\theta_E}\right)^{m_E k} \\ \Psi\left(m_E, m_E+1+i, \frac{\rho-1}{\rho}\left(\frac{\rho(P_0\epsilon^2 p+1)}{P_0\theta_D}+\frac{P_0\epsilon^2+1}{P_0\theta_E}\right)\right)^k. \tag{11}$$

where $\Psi(\cdot)$ is the confluent hypergeometric function defined in [15, (2.3.6.9)].

In this section, we obtain the SOP of the considered system over i.i.d Nakagami-m fading channel under the both uncertainties from wireless backhaul and channel estimation. We also propose a novel OS scheme for small-cell networks to combat these imperfections.

IV. Asymptotic analysis

In order to gain further insights into secure small-cell networks, we also study asymptotic behaviours in the high SNR regime under the imperfections of wireless backhaul and channel estimation.

In the high SNR regime, we assume that $P_0 \to \infty$, and the asymptotic limits of (11) can be expressed as:

$$\mathbb{P}_{\substack{\text{out}\\P_0\to\infty}}^{SS} \approx 1 + \sum_{k=1}^{K}\binom{K}{k}(-1)^k p^k \exp\left(-\frac{\epsilon^2 p}{\theta_D}k(\rho-1)\right) \\ \sum_{w_1+w_2+\ldots+w_{m_D}=k}\frac{k!}{w_1!w_2!\ldots w_{m_D}!} \\ \frac{(\rho-1)^{\sum_{t=0}^{m_D-1}tw_{t+1}}}{\prod_{t=0}^{m_D-1}\left(t!\left(\frac{\theta_D}{\epsilon^2 p}\right)^t\right)^{w_{t+1}}}\left(\frac{\epsilon^2}{\theta_E}\right)^{m_E k}\left(\frac{\rho-1}{\rho}\right)^{m_E k} \\ \Psi\left(m_E, m_E+1+i, \frac{\rho-1}{\rho}\left(\frac{\rho\epsilon^2 p}{\theta_D}+\frac{\epsilon^2}{\theta_E}\right)\right)^k. \tag{12}$$

Apparently, the asymptotic behaviour does not depend on P_0 in the high SNR regime. The validation of our theoretical analysis are provided in the next section.

V. Numerical and Simulation Results

We give numerical and simulation findings to demonstrate the system secrecy performance under the wireless backhaul imperfections and channel estimation errors by Monte Carlo simulations. We present the simulation results of our proposed OS scheme, and also compare the system secrecy performance between OS and another two selection schemes: Sub-optimal small-cell transmitter Selection (SS) which optimizes the secrecy capacity of legitimate channel and Minimum-Eavesdropping small cell transmitter Selection (MES) which

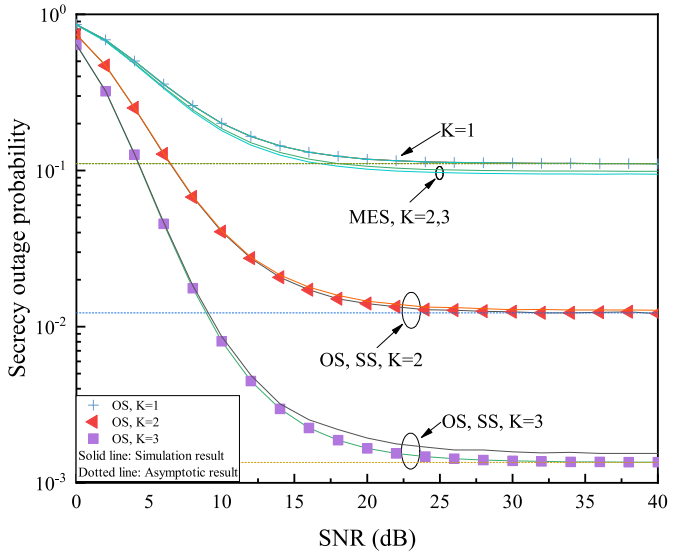

Fig. 2. Comparison of OS, SS and MES on the impacts of the number of K on SOP for K=1, 2, 3 with unreliable backhaul (p=0.95) and imperfect channel estimation (ϵ^2=0.1)

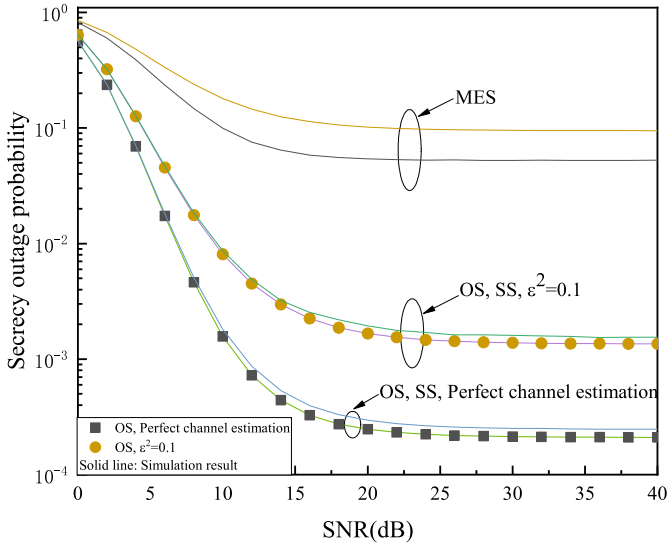

Fig. 3. Comparison of imperfect channel estimation error (ϵ^2=0.1) and perfect channel estimation (ϵ^2=0) on SOP with p=0.95 and K=3 for SS, OS and MES.

combats eavesdropping. Our results show the superiority of our proposed OS scheme under the practical constraints of wireless backhaul and channel estimation.

The following parameters are fixed for simulation. The threshold for SOP is θ=1 bits/s/Hz; the m parameter is $m_E = 2$ and $m_D = 2$, respectively. We also assume that the nodes' locations in Cartesian coordinate system are T_k=(0, 0), $\forall$ k, D=(1, 0), E=(2, 2). Additionally, the average SNR of each link is assumed to depend on path loss, given as $\frac{1}{\Omega_X} = \frac{1}{d_X^p}$, where the path loss exponent p is assumed to equal 4, and d_X is the distance between two nodes. In the following figures, the lines, the markers and the dotted lines represent the simulation, theoretical and asymptotic results, respectively. We could observe from the figures that our novel theoretical results match the simulation curves, therefore validating the correctness of theoretical analysis in Section III and Section IV.

Fig. 2 plots the SOP versus SNR (P_0) for the different number of small-cell transmitters K, K=1, K=2 and K=3. The network parameters are set as p=0.95 and ϵ^2=0.1. We show the theoretical and simulation results of our proposed OS scheme. In addition, we also compare the performance between OS and another two benchmark schemes: SS and MES. As we can see from the figure that OS has the best performance, SS has the second best performance and MES performs the worst. This proves the superiority of the proposed OS scheme under the unreliable backhaul and imperfect channel estimation. The OS scheme outperforms the other schemes because it requires the knowledge of global CSI and wireless backhaul. The secrecy performance of the SS scheme is inferior to OS since it only needs legitimate CSI and backhaul activity. MES has the poorest performance as only CSI of the wiretap channel is utilized during the selection. The comparison of these selection schemes demonstrate that the system could achieve better secrecy performance if more information is provided.

We could also observe from Fig. 2 that an increase in P_0 could enhance SOP in the low SNR regime, and the SOP reaches the asymptotic limits eventually in the high SNR regime. This is due to the fact that as P_0 rises, the transmit power of the small-cell transmitter rises as well, thus improving the secrecy performance. The asymptotic behaviour shows that the performance of the considered system is constrained by K, p, ϵ^2 and the other channel parameters. Moreover, when there are more small-cell transmitters, the system could achieve higher diversity. Therefore, a larger K could enhance the system secrecy performance for all selection schemes at different levels. To be specific, the OS and SS schemes improve the secrecy performance significantly because of the increased likelihood of choosing a small-cell transmitter with better channel conditions. However, MES only shows limited decrement of SOP with an increase of K. This is due to the fact that the SOP depends on the probability that the quality of legitimate channel outperforms the wiretap channel. Despite the rises of K increases the likelihood to combat eavesdropping in MES, the legitimate channel from the small-cell transmitter to the destination is not optimized compared to the other two schemes. This results in the worst secrecy performance of the MES scheme.

Fig. 3 represents the influence of channel estimation errors on the secrecy performance. The figure plots the SOP under perfect channel estimations, $\epsilon^2 = 0$, and imperfect channel estimation with $\epsilon^2 = 0.1$, when p=0.95 and K=3. MES shows the worst performance, and OS slightly outperforms SS. It is clearly shown that the SOP with perfect channel estimation is significantly lower than that with imperfect channel estimation.

Fig. 4 shows the SOP versus P_0 for different backhaul

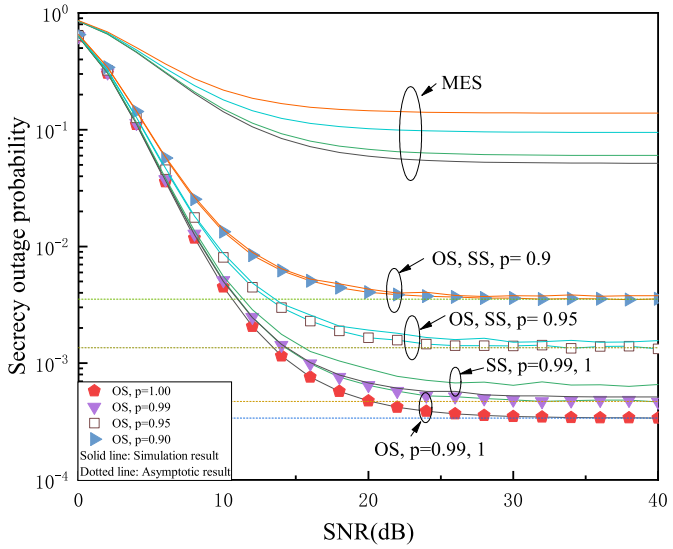

Fig. 4. Impact of backhaul reliability on SOP for $p = 0.9$, $p = 0.95$, $p = 0.99$ and $p = 1.00$ with $K = 3$ and $\epsilon^2 = 0.1$ for SS, OS and MES.

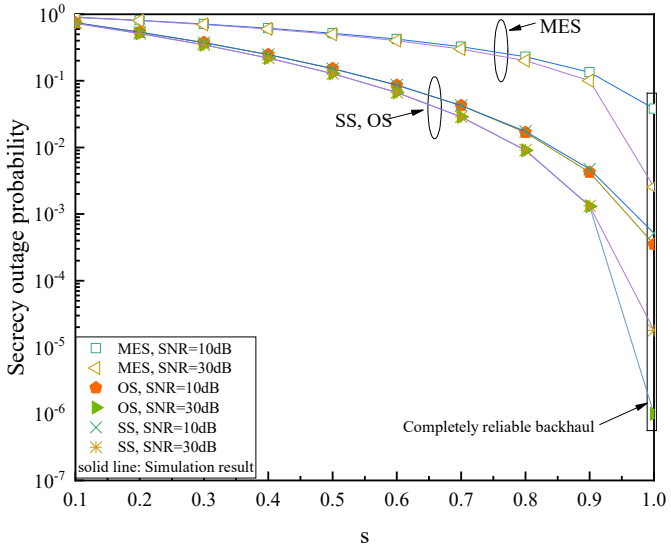

Fig. 5. Impact of backhaul reliability on SOP with P_0=10 dB and P_0=30 dB for the three selection schemes: SS, OS and MES.

reliability values, $p = 0.90$, $p = 0.95$, $p = 0.99$, and perfect backhaul condition $p = 1.00$. The network parameters are set as $K = 3$ and $\epsilon^2 = 0.1$. Similar to previous figures, the MES scheme shows the worst performance. We could also observe that SOP decreases and converges to a constant value with the increase of p. The system with more reliable backhaul shows better performance. The figure also proves that the backhaul reliability p is responsible for the asymptotic behaviour.

Similar patterns could be seen in Fig. 5 where the SOP versus p is plotted for the three schemes with different values of P_0, i.e., P_0=10 dB and P_0=30 dB. The SOP decreases for all three schemes when the backhaul is more reliable and achieves the lowest point when the backhaul is perfect. This shows that wireless backhaul reliability has significant impacts on system performance and should be considered in future heterogeneous system designs.

VI. Conclusion

In this paper, we have derived the exact and asymptotic secrecy outage probability of the small-cell networks with the best small-cell selection scheme over i.i.d. Nakagami-m fading channels. We also compared the proposed scheme with some benchmarks, such as the sub-optimal scheme and minimum eavesdropping scheme to highlight the advantage of using the best small cell in coping with the eavesdroppers in physical layer security. Our numerical results demonstrated that the unreliable backhaul and channel estimation error played a significant role in the performance of small networks. As such, wireless system designers must pay attention to these practical aspects when investigating the performance of small-cell networks.

References

[1] C. Yin, Z. Su, and A. Kortun, "Performance analysis of cognitive vehicular networks under unreliable backhaul," *EAI Endorsed Trans. Ind. Netw.*, vol. 8, no. 26, Apr. 2021.

[2] M. Coldrey, H. Koorapaty, J.-E. Berg, Z. Ghebretensae, J. Hansryd, A. Derneryd, and S. Falahati, "Small-cell wireless backhauling: A non-line-of-sight approach for point-to-point microwave links," in *2012 IEEE Veh. Technol. Conf. (VTC Fall)*. IEEE, 2012, pp. 1–5.

[3] T. T. Tran, "Network-coding-based jamming with triple transmission time slots: A method to secure transmission in an extreme case of source-wiretapping and unshared jamming signal," *EAI Endorsed Trans. Ind. Netw.*, vol. 8, no. 27, p. e5, 2021.

[4] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Aca. Sci.*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

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

[6] C. Yin, X. Cheng, Y. Li, and H. Liu, "Impact of wireless backhaul and imperfect channel estimation on secure communication networks," in *Int. Conf. Industr. Netw. Intell. Syst.* Springer, 2022, pp. 231–240.

[7] H. T. Nguyen, J. Zhang, N. Yang, T. Q. Duong, and W.-J. Hwang, "Secure cooperative single carrier systems under unreliable backhaul and dense networks impact," *IEEE Access*, vol. 5, pp. 18 310–18 324, Jul. 2017.

[8] C. Yin, H. T. Nguyen, C. Kundu, Z. Kaleem, E. Garcia-Palacios, and T. Q. Duong, "Secure energy harvesting relay networks with unreliable backhaul connections," *IEEE Access*, vol. 6, pp. 12 074–12 084, Jan. 2018.

[9] M. Nakagami, "The m-distribution—A general formula of intensity distribution of rapid fading," in *Statistical methods in radio wave propagation*. Elsevier, Jun. 1960, pp. 3–36.

[10] C. Yin, E. Garcia-Palacios, N.-S. Vo, and T. Q. Duong, "Cognitive heterogeneous networks with multiple primary users and unreliable backhaul connections," *IEEE Access*, vol. 7, pp. 3644–3655, 2018.

[11] C. Yin, N.-P. Nguyen, E. Garcia-Palacios, X. N. Tran, and T. Le-Tien, "Secure energy harvesting communications with relay selection over Nakagami-m fading channels," *Mob. Netw. Appl.*, vol. 23, no. 6, pp. 1555–1562, 2018.

[12] I. S. Gradshteyn and I. Ryzhik, "Table of Integrals, Series, and Products. 7th ed." *Elsevier/Academic Press, Amsterdam*, vol. 48, p. 1171, 2007.

[13] N. T. Anh, N. C. Minh, T. T. Duy, T. Hanh, and H. D. Hai, "Reliability-security analysis for harvest-to-jam based multi-hop cluster MIMO networks using cooperative jamming methods under impact of hardware impairments," *EAI Endorsed Trans. Ind. Netw.*, vol. 8, no. 28, Sep.2021.

[14] T. T. Duy, L. C. Khan, N. T. Binh, and N. L. Nhat, "Intercept probability analysis of cooperative cognitive networks using fountain codes and cooperative jamming," *EAI Endorsed Trans. Ind. Netw.*, vol. 8, no. 26, Jan. 2021.

[15] A. P. Prudnikov, Y. A. Brychkov, O. I. Marichev, and R. H. Romer, "Integrals and Series," 1988.