Physical Layer Security of Heterogenous Networks with Unreliable Wireless Backhaul and Small Cell Selections

Eoin O'Boyle[1(✉)], Xinkai Cheng[2], and Cheng Yin[3]

[1] Queen's University, Belfast, UK
eoboyle11@qub.ac.uk
[2] Wuhan University of Science and Technology, Wuhan, China
[3] University of Surrey, Guildford, UK
c.yin@surrey.ac.uk

Abstract. In this study, we propose a novel secure heterogeneous network system model that incorporates an unreliable wireless backhaul and perfect channel estimation across identical Rayleigh fading channels. Our approach employs three transmission schemes: Sub-Optimum Selection (SS), Optimum Selection (OS), and Minimum-Eavesdropping Selection (MES), with the goal of improving the secrecy performance of the system. We derive advanced closed-form expressions for the Secrecy Outage Probability (SOP) for these three selection schemes in both practical and ideal scenarios. We investigate the influence of uncertainties in wireless backhaul and perfect Channel State Information (CSI) on the system's secrecy performance. Furthermore, we examine how the number of small-cell transmitters impacts the system's secrecy performance. By conducting Monte-Carlo simulations, we validate the accuracy of our analytical results. This verification ensures the correctness of our expressions and strengthens the reliability of our findings.

Keywords: Physical layer security · Rayleigh fading · Secrecy outage probability · Wireless backhaul

1 Introduction

Physical layer security has been considered as a promising technology to build the security of wireless networks [1]. The fundamental concept behind physical layer security involves leveraging the inherent properties of wireless channels to ensure message security from an information-theoretical perspective. A seminal study by Wyner demonstrated that when the primary channel between the source and destination surpasses the eavesdropping channel, it is possible to achieve flawless message security at a nonzero transmission rate. In this context, employing small cell transmitter selection schemes proves to be an efficient approach [2–6].

The rising wireless data traffic demand leads networks being more dense and heterogeneous. Heterogeneous networks supply effective methods of accommodating current

N.-S. Vo and H.-A. Tran (Eds.): INISCOM 2023, LNICST 531, pp. 315–326, 2023.
https://doi.org/10.1007/978-3-031-47359-3_23

data traffic growth by building macro base stations with small-cells and access points [6]. Macro base stations are typically erected on towers to facilitate extensive transmission coverage using low-frequency bands. On the other hand, small cells operate on higher frequency bands and offer radio coverage within a shorter range compared to macro cells. Despite their smaller coverage area, small cells provide highly reliable connections characterized by low latency and high speed. In order to meet the increasing data traffic demands, both macro base stations and small cells are integrated to create heterogeneous networks. These networks are designed to address future communication requirements. The backhaul plays a crucial role by establishing connections between the macro base station and the small cells. Wireless backhaul has emerged as a solution for establishing communication connections between small cells and access points in outdoor where wired connections are not avaliable. Although wireless backhaul encounters occasional unreliability, it has proven to be a viable method for ensuring seamless communication in such scenarios [11]. The deployment of a two-tier network configuration was explored, involving a macro base station that establishes a connection with the cloud. In this setup, small cells have the capability to connect wirelessly to either the macro base station or the core network by utilizing backhaul links [11–13]. The demand for high connectivity in heterogeneous networks has led to a proliferation of devices, thereby posing significant challenges to wireless security. Furthermore, the inherent uncertainties in wireless communication make these networks even more susceptible to various attacks. Consequently, the research focus has shifted towards exploring secure heterogeneous networks that can effectively address the issue of wireless backhaul unreliability.

In this paper, we assume that transmission links follow Rayleigh fading channel, which is a special case of Nakagami-*m* fading [14]. Additionally, we propose different transmitter selection schemes to enhance the secrecy performance under perfect channel estimation and wireless backhaul uncertainties. This study proposes an advanced design for a secure heterogeneous system based on Physical Layer Security (PLS). The investigation focuses on the impact of unreliable wireless backhaul and perfect channel estimation in the presence of Rayleigh fading. To enhance the secrecy performance of the system, three small-cell transmitter selection schemes are introduced: SS, OS and MES. These selection schemes are implemented to improve the overall security of the system.

2 System Model

The considered system model is in Fig. 1. It consists of K small-cells transmitters, $\{T_1,\ldots, T_k,\ldots, T_K\}$, connecting to a macro-base station, BS, through unreliable backhaul links, b_k, a secondary destination, D, and an eavesdropper, E. We assume T − D and undergo independent and identically distributed Rayleigh fading [2].

The best transmitter is chosen among K small-cell transmitters in the considered system. When the information is sent to small-cell transmitters, there is a certain probability that the backhaul fails to convey the transmission. We model the backhaul reliability as a Bernoulli process, I_k. The success probability of Bernoulli process is defined as s, and failure probability is defined as 1 – s [6].

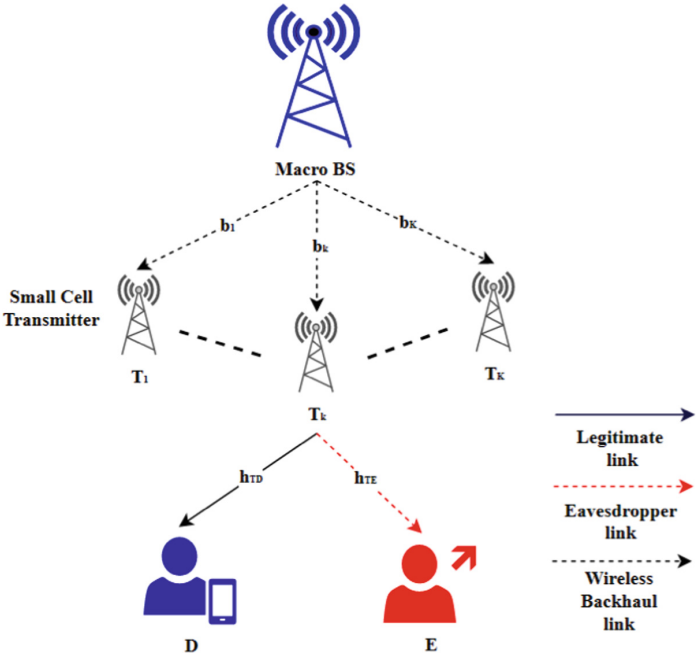

Fig. 1. Secure heterogenous network.

The CDF and PDF of the random variable X is

$$F_X(x) = 1 - exp\left(-\frac{x^2}{2\sigma^2}\right), for\ x \in [0, \infty]$$
$$f_X(x) = \frac{x}{\sigma^2} exp\left(-\frac{x^2}{2\sigma^2}\right), for\ x \geq 0 \tag{1}$$

The connection between the small-cell transmitters and the macro BS is established through backhaul. The received signals at D and E can be expressed as follows:

$$\begin{aligned} Fy_D &= \sqrt{P_T} h_{T_k D} \mathbb{I}_k x + z, \\ y_E &= \sqrt{P_T} h_{T_k E} x + z, \end{aligned} \quad F \tag{2}$$

where $h_{T_{kD}}$ and $h_{T_k E}$ are channel coefficients from T_k to D and from T_k to E. In addition, x is the power transmitted symbol and P_T is the transmitted power of T_k. It is assumed that D and E encounter the complex additive white Gaussian Noise, i.e., $z \sim CN\left(0, \sigma^2\right)$. The relationship between the estimated channel coefficients $\hat{h}_{T_k D}$, $\hat{h}_{T_k E}$ and real channel coefficients $h_{T_k D}$, $h_{T_k E}$ are given as

$$\begin{aligned} \hat{h}_{T_k D} &= h_{T_k D}, \\ \hat{h}_{T_k E} &= h_{T_k E}. \end{aligned} \tag{3}$$

Then, the received signals are rewritten as

$$y_D = \sqrt{P_T}\hat{h}_{T_kD}\mathbb{I}_k x + z,$$
$$y_E = \sqrt{P_T}\hat{h}_{T_kE}x + z. \tag{4}$$

In consonance with (4), the SNRs at D and E are,

$$SNR_{TD} = \frac{P_T|h_{TD}|^2\mathbb{I}_k}{\sigma^2} = \gamma_m|h_{TD}|^2\mathbb{I}_k,$$
$$SNR_{TE} = \frac{P_T|h_{TE}|^2}{\sigma^2} = \gamma_m|h_{TE}|^2, \tag{5}$$

where $\gamma_m = \frac{P_T}{\sigma^2}$. To improve the system secrecy performance, the best transmitter T_{k^*} is chosen from the K transmitters. The SNRs at D and E with the selected T_{k^*} are

$$SNR_{T_{k^*}D} = \frac{P_T\left|h_{T_{k^*}D}\right|^2\mathbb{I}_{k^*}}{\sigma^2} = \gamma_m\left|h_{T_{k^*}D}\right|^2\mathbb{I}_{k^*},$$
$$SNR_{T_{k^*}E} = \frac{P_T\left|h_{T_{k^*}E}\right|^2}{\sigma^2} = \gamma_m\left|h_{T_{k^*}E}\right|^2, \tag{6}$$

where $\left|h_{T_{k^*}D}\right|^2$ and $\left|h_{T_{k^*}E}\right|^2$ are the channel coefficients of the chosen transmitter T_{k^*} to D and E. $\mathbb{I}_{k^*}$ represents the backhaul reliability from the macro-BS to T_{k^*}.

3 Small Cell Transmitter Selection Schemes

This section presents the three small-cell selection schemes, which are expressed as follows.

A. *Sub-optimum Selection (SS)*

By using T_k-D links, the SS scheme chooses the transmitter by calculating the maximum power gain as

$$k^* = arg\max_{1\le k\le K}\gamma_m\left|h_{T_kD}\right|^2\mathbb{I}_k, \tag{7}$$

where k^* indicates the index of the chosen transmitter.

B. Optimum Selection (OS)

The OS requires global CSI of the considered system and the system secrecy capacity is given as

$$C_s = \left[log_2(1 + SNR_{TD}) - log_2(1 + SNR_{TE})\right]^+, \tag{8}$$

where $[x]^+$=max $(x, 0)$ and the definitions of SNR_{TD} and SNR_{TE} are illustrated in (5).

$$k^* = argmaxC_s^k, \tag{9}$$

where $C_s^k = \left[log_2\left(1 + SNR_{T_{k^*}D}\right) - log_2\left(1 + SNR_{T_{k^*}E}\right)\right]^+$ and the definitions of $SNR_{T_{k^*}D}$ and $SNR_{T_{k^*}E}$ can be found in (6).

C. Minimum-Eavesdropping Selection (MES)

The MES scheme is considered to select the smallest channel gain from T_k to E. The transmitter T_{k^*} is chosen by searching the worst $T_k - E$ link. This scheme can be written mathematically as

$$k^* = arg \min_{1 \le k \le K} \left| h_{T_k E} \right|^2. \tag{10}$$

4 Performance Analysis

The system performance is analysed by deriving SOP expressions including uncertainties from wireless backhaul unreliability. The definition of SOP is mathematically written as [8]

$$\begin{aligned} \mathbb{P}_{out}(\theta) &= \mathbb{P}_{out}(C_s < \theta) \\ &= \int_0^{\infty} F_{T_{k^*}D}(\rho(1+x)-1) f_E(x) dx. \end{aligned} \tag{11}$$

where $F_{T_{k^*}D}(\rho(1+x)-1)$ is the CDF, $f_E(x)$ is the PDF and $\rho = 2^{\theta}$.

The CDF and PDF of random variable $\mathbb{I}_k X$ for the $T - D$ link is given as

$$\begin{aligned} F_{|h_{TD}|^2 \mathbb{I}_k X}(x) &= \int_0^{t} (1-s)\delta(x) + s\lambda_{TD} exp(-\lambda_{TDx}) dt. = 1 - sexp\left(-\lambda_{TD} \frac{x}{\gamma_m}\right) \\ f_{|h_{TD}|^2 \mathbb{I}_k X}(x) &= (1-s)\delta(x) + s\lambda_{TD} exp(-\lambda_{TDx}) \end{aligned} \tag{12}$$

The PDF expression of random variable $\mathbb{I}_k$X for the T-E link is

$$f_E(x) = \frac{\lambda_{TE}}{\gamma_m} exp\left(-\lambda_{TE} \frac{x}{\gamma_m}\right) \tag{13}$$

where $\gamma_m = P_T / \sigma^2$.

1) ***Sub-optimum Selection:***

Firstly, we derive the SOP of the SS scheme. Conforming to the selection rules in (7), the SOP expression of the SS scheme is,

$$\begin{aligned} \mathbb{P}_{out}(\theta) &= \mathbb{P}_{out}(C_s < \theta) \\ &= \int_0^{\infty} F_{T_{k^*}D}(\rho(1+x)-1) f_E(x) dx. \end{aligned} \tag{14}$$

The CDF and PDF are,

$$F_{T_k^* D} = F_{TD}^k = \left[1 - sexp\left(-\lambda_{TD} \frac{x}{\gamma_m}\right)\right]^k$$

$$= 1 + \sum_{k=1}^{K} (-1)^k \binom{K}{k} s^k exp\left(-\frac{\lambda_{TD} kx}{\gamma_m}\right) \tag{15}$$

Substituting this equation into $\mathbb{P}_{\text{out}}(\theta)$ leads to the corresponding CDF,

$$F_{T_{k^*D}}(\rho(1+x)-1) = 1 + \sum_{k=1}^{K} (-1)^k \binom{K}{k} s^k exp\left(-\frac{\lambda_{TD} k(\rho(1+x)-1)}{\gamma_m}\right)$$

The PDF part is written mathematically as,

$$f_E(x) = \frac{\lambda_{TE}}{\gamma_m} exp\left(-\lambda_{TE}\frac{x}{\gamma_m}\right)$$

Therefore, the final SOP of the SS scheme is given as,

$$\mathbb{P}_r(C_s < \theta) = \int_0^{\infty} 1 + \sum_{k=0}^{K} \binom{K}{k} (-1)^k s^k exp\left(-\frac{\lambda_{TD} k(\rho(1+x)-1)}{\gamma_m}\right) \frac{\lambda_{TE}}{\gamma_m} exp\left(-\lambda_{TE}\frac{x}{\gamma_m}\right)$$

$$= 1 + \sum_{k=0}^{K} \binom{K}{k} (-1)^k s^k \tfrac{\lambda_{TE}}{\gamma_m} \int_0^{\infty} exp\left(-\tfrac{\lambda_{TD} k(\rho(1+x)-1)}{\gamma_m}\right) exp\left(-\lambda_{TE}\tfrac{x}{\gamma_m}\right)$$
$$= 1 + \sum_{k=0}^{K} \binom{K}{k} (-1)^k s^k \tfrac{\lambda_{TE}}{\gamma_m} \int_0^{\infty} exp\left(-\tfrac{\lambda_{TD} k(\rho(1+x)-1)-\lambda_{TE} x}{\gamma_m}\right)$$
$$= 1 + \sum_{k=0}^{K} \binom{K}{k} (-1)^k s^k \tfrac{\lambda_{TE}}{\gamma_m} \tfrac{\gamma_m}{\lambda_{TD}\rho k + \lambda_{TE}} exp\left(-\tfrac{\lambda_{TD} k(\rho(1+0)-1)-\lambda_{TE}(0)}{\gamma_m}\right)$$
$$= 1 + \sum_{k=0}^{K} \binom{K}{k} (-1)^k s^k \tfrac{\lambda_{TE}}{\gamma_m} \tfrac{\gamma_m}{\lambda_{TD}\rho k + \lambda_{TE}} exp\left(-\tfrac{\lambda_{TD}\rho k - \lambda_{TD} k}{\gamma_m}\right)$$

Thus, the SOP for SS is written mathematically as,

$$\mathbb{P}_{\boldsymbol{out}}^{\boldsymbol{SS}} = 1 + \sum_{\boldsymbol{k=0}}^{\boldsymbol{K}} \binom{\boldsymbol{K}}{\boldsymbol{k}} (-1)^{\boldsymbol{k}} \boldsymbol{s}^{\boldsymbol{k}} \left(\frac{\boldsymbol{\lambda_{TE}}}{\boldsymbol{\lambda_{TD}\rho k + \lambda_{TE}}}\right) \boldsymbol{exp}\left(-\frac{\boldsymbol{\lambda_{TD} k\rho - \lambda_{TD} k}}{\boldsymbol{\gamma_m}}\right) \tag{16}$$

2) ***Optimum Selection:***

Firstly, the CDF and PDF of the OS scheme are,

$$F_{TD} = 1 - sexp\left(-\lambda_{TD}\frac{x}{\gamma_m}\right)$$
$$f_E(x) = \frac{\lambda_{TE}}{\gamma_m} exp\left(-\frac{\lambda_{TE} x}{\gamma_m}\right) \tag{17}$$

Then, substituting the above equations into (11) and we can obtain the following integral,

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

$$= \int_0^{\infty} \left[1 - sexp\left(-\lambda_{TD}\frac{(\rho(1+x)-1)}{\gamma_m}\right)\right]\frac{\lambda_{TE}}{\gamma_m}exp\left(-\lambda_{TD}\frac{\lambda_{TE}x}{\gamma_m}\right)dx.$$

$$= 1 - s\frac{\lambda_E}{\gamma_m}exp\left(\frac{-\lambda_{TD}}{\gamma_m}\rho + \frac{\lambda_{TD}}{\gamma_m}\right)\int_0^{\infty} exp\left(-\frac{\lambda_{TD}}{\gamma_m}\rho x - \frac{\lambda_E}{\gamma_m}\right)dx.$$

Recall the selection rules in (9), we obtain

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

$$= \left[1 - \frac{s\lambda_E}{\lambda_{TD}\rho + \lambda_{TE}}exp\left(-\frac{\lambda_{TD}\rho + \lambda_{TD}}{\gamma_m}\right)\right]^k$$

The SOP of the OS scheme is expressed as

$$\mathbb{P}_{\boldsymbol{out}}^{\boldsymbol{OS}} = \sum_{\boldsymbol{k}=0}^{\boldsymbol{K}} \binom{\boldsymbol{K}}{\boldsymbol{k}} (-1)^{\boldsymbol{k}} \boldsymbol{s}^{\boldsymbol{k}} \left(\frac{\boldsymbol{\lambda_{TE}}}{\boldsymbol{\lambda_{TD}\rho + \lambda_{TE}}}\right)^{\boldsymbol{k}} \boldsymbol{exp}\left(-\frac{\boldsymbol{\lambda_{TD}k\rho + \lambda_{TD}k}}{\boldsymbol{\gamma_m}}\right) \tag{18}$$

3) ***Minimum Eavesdropping Selection:***

The CDF and PDF of the MES scheme are:

$$F_{TD} = 1 - sexp\left(-\lambda_{TD}\frac{x}{\gamma_m}\right)$$

$$f_E(x) = \frac{\lambda_{TE}}{\gamma_m}kexp\left(-\frac{\lambda_{TE}}{\gamma_m}kx\right) \tag{19}$$

Based on the selection rule of the MES scheme in (10) we could obtain

$$\mathbb{P}_r(C_s < \theta) = \int_0^{\infty} (1 - sexp(-\lambda_{TD}\frac{(\rho(1+x)-1)}{\gamma_m})\frac{\lambda_{TE}k}{\gamma_m}exp\left(-\frac{\lambda_{TE}}{\gamma_m}kx\right)dx.$$

$$= 1 - s\frac{\lambda_{TE}k}{\gamma_m}\int_0^{\infty} exp(-\lambda_{TD}\frac{(\rho(1+x)-1)}{\gamma_m})exp\left(-\frac{\lambda_{TE}}{\gamma_m}kx\right)dx.$$

$$= 1 - s\frac{\lambda_{TE}k}{\gamma_m}\int_0^{\infty} exp(-\lambda_{TD}\frac{(\rho(1+x)-1)-\lambda_{TE}kx}{\gamma_m})dx.$$

$$= 1 - s\frac{\lambda_{TE}k}{\gamma_m}\frac{\gamma_m}{\lambda_{TD}\rho + \lambda_{TE}k}exp\left(-\frac{\lambda_{TD}(\rho(1+0)-1)-\lambda_{TE}k(0)}{\gamma_m}\right)$$

$$= 1 - \left(\frac{s\lambda_{TE}k}{\lambda_{TD}p + \lambda_{TE}k}\right)exp\left(-\frac{\lambda_{TD}p + \lambda_{TD}}{\gamma_m}\right)$$

The closed-form expression of the MES scheme is obtained as

$$\mathbb{P}_{\boldsymbol{out}}^{\boldsymbol{MES}} = 1 - \left(\frac{\boldsymbol{s\lambda_{TE}k}}{\boldsymbol{\lambda_{TD}\rho + \lambda_{TE}k}}\right)\boldsymbol{exp}\left(-\frac{\boldsymbol{\lambda_{TD}\rho + \lambda_{TD}}}{\boldsymbol{\gamma_m}}\right) \tag{20}$$

5 Numerical and Simulation Results

We employ Monte Carlo simulations to illustrate the numerical and simulation outcomes, showcasing the system's secrecy performance in the presence of wireless backhaul uncertainties and perfect channel estimation. Additionally, we conduct a comparative analysis of the system's secrecy performance across different selection schemes in both practical and ideal scenarios. By comparing the simulation curves and the analysis results, we observe a close correspondence, thereby validating the accuracy and reliability of our theoretical analysis. Threshold, θ, is set at 1bits/s/Hz. We assume that transmitters, receiver and eavesdropper are located at $T_k = (0,0)$, $D = (1,0)$ and $E = (4,1)$ in Cartesian coordinate system. The path loss pl is assumed as 4 [10].

Figure 2 below presents SOP against SNR (γ_m). Parameter s is set at 0.99. Among the selection schemes considered, the OS outperforms the others due to its utilization of global CSI and wireless backhaul information. This comprehensive approach results in superior secrecy performance. On the other hand, the SS scheme, which only relies on partial CSI combined with backhaul information, exhibits lower secrecy performance compared to the OS scheme. The MES scheme performs poorly as it solely relies on the CSI of the wiretap channel. Generally, system performance is hindered by K, s, and the other parameters, reaching the asymptotic limits eventually. The secrecy performance for all schemes improves with an increase in the parameter K, as it enhances the achieved diversity by increasing the number of small cell transmitters. Both the SS and OS schemes exhibit remarkable enhancements in secrecy performance due to a higher likelihood of selecting a small-cell transmitter with superior channel conditions. However, the MES scheme shows only marginal improvement with an increase in the number of small-cell transmitters. The SOP relies on the probability that the legitimate channel possesses better quality than the wiretap channel. While increasing K results in a higher probability of selecting a weaker channel for the eavesdropper in the MES scheme, it does not lead to an improvement in the main channel from the small-cell transmitter to the destination, unlike the other two schemes. As a result, the MES scheme does not exhibit a clear overall enhancement in secrecy performance.

Figure 3 shows SOP versus γ_m for different backhaul reliability values. Similar to Fig. 2, the MES scheme demonstrates the poorest performance among the three schemes. It is evident that the SOP experiences a sudden decrease for the SS and OS schemes, while it decreases gradually for the MES scheme and eventually converges to a constant value at approximately 30dB for all schemes.

Figure 4 shows the impact of the distance between the E and T_k, d_{T_kE}, on SOP with parameters, K = 3 and s= 0.90. We assume that, d_{T_kD}, is unity as d_{T_kD}=1.0. We consider the following four cases: 1. d_{T_kE}= 1.0; 2. d_{T_kE} = 2.0; 3. d_{T_kE} = 10.0; 4. d_{T_kE} = 0.5. In these sets of parameters, we observe from *Fig. 4* that the SOP decreases when the eavesdropper locates further from the transmitter.

Moreover, SOP exhibits significantly high values when the distance between T_k and E is equal to or smaller than that between T_k and D, at distances of 0.5 and 1.0. This implies that the wiretap channel quality surpasses that of the legitimate channel. On the contrary, PLS can be achieved when E is positioned further to T_k than D. As outlined in Fig. 4, it is evident that the OS scheme outperforms the SS scheme due to the additional channel knowledge utilized in the proposed system. Notably, when the distance between

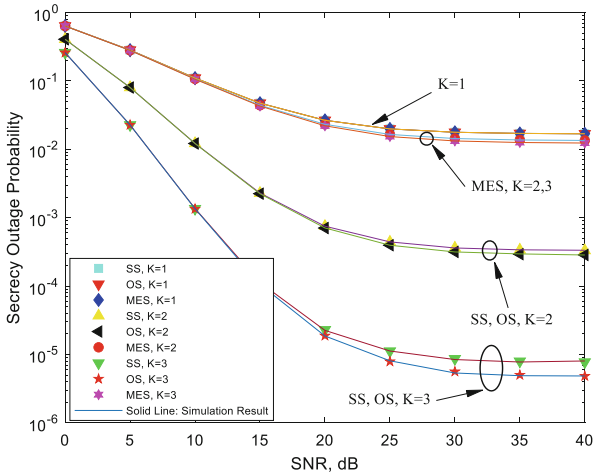

Fig. 2. Impact of number of K on SOP for K = 1, 2, 3.

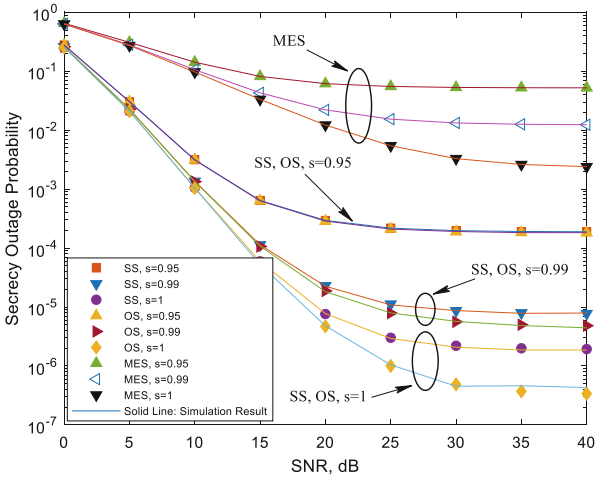

Fig. 3. Impact of backhaul reliability on SOP for s = 0.95, s = 0.99 and s = 1.00.

E and T_k becomes extremely large ($d_{T_kE} = 10.0$), the SOP curves of SS and OS nearly coincide. This indicates that considering the wiretap CSI in the transmitter selection has minimal impact on enhancing the secrecy performance when the wiretap channel quality is severely inadequate, such as when E is located far away from T_k.

The SOP versus s is provided with various values of P_o, i.e., P_o=5 dB and P_o=30 dB in Fig. 5. As the reliability of the backhaul increases, the SOP decreases for all three schemes, reaching its minimum when the backhaul is perfect. This observation underscores the significant impact of wireless backhaul reliability on system performance. Consequently, it becomes crucial to account for this imperfection when designing future heterogeneous system models.

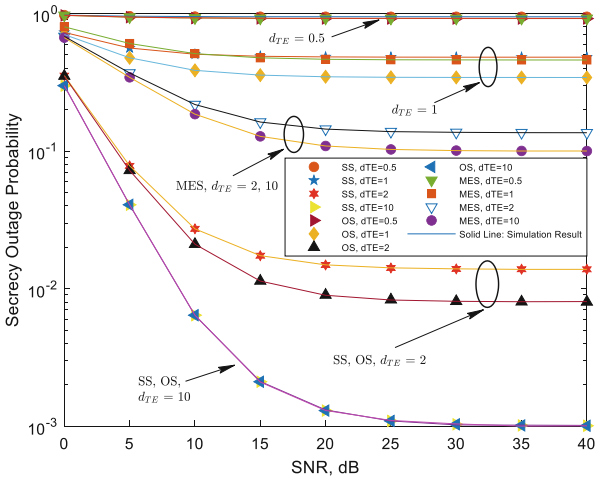

Fig. 4. Impact of different distances between T and E on SOP: d_{TE}=0.5, 1, 2 and 1.

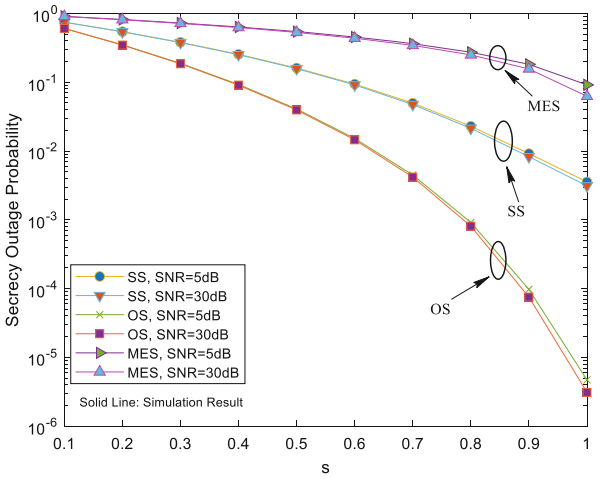

Fig. 5. Impact of backhaul reliability on SOP with $Po = 5$ dB and $Po = 30$ dB.

6 Conclusion

We evaluated the effectiveness of a heterogeneous network incorporating an unreliable backhaul in maintaining secrecy by proposing three transmitter selection schemes for small-cell networks. We derived closed-form expressions for the SOP and investigated the impact of uncertain backhaul connections on the network's ability to maintain secrecy. Our innovative theoretical analysis and simulations demonstrated that the OS scheme outperformed the SS scheme in scenarios where additional CSI knowledge was available. However, this advantage diminished significantly when the quality of the

wiretap channel was extremely poor. Conversely, the MES scheme exhibited the weakest performance as it relied solely on the channel knowledge of the eavesdropper's link. Furthermore, increasing the number of small-cell transmitters had a positive impact on the system's secrecy performance with the OS and SS schemes. However, the MES scheme showed minimal sensitivity to changes in the number of small-cell transmitters. Additionally, the influence of wireless backhauls impairments on the system's secrecy performance varied depending on the number of small-cell transmitters in the SS and OS schemes. In contrast, the MES scheme demonstrated less susceptibility to the number of small-cell transmitters.

References

1. Tang, W., Feng, S., Ding, Y., Liu, Y.: Physical layer security in heterogeneous networks with jammer selection and full-duplex users. IEEE Trans. Wireless Commun. **16**(12), 7982–7995 (2017)
2. Yin, C., Duong, T.Q., Xiao, P.: Secrecy performance of small-cell networks over nakagami-m fading in the presence of unreliable backhaul and imperfect CSI. IEEE 18th International Conference on Wireless and Mobile Computing, Networking and Communication, pp. 257–261 (2022)
3. Yin, C., Garcia-Palacios, E., Xiao, P., Sharma, V., Dobre, O.A., Duong, T.Q.: Secrecy performance analysis of heterogeneous networks with unreliable wireless backhaul and imperfect channel estimation. IEEE Transactions on Vehicular Technology (2023)
4. Kotwal, S.B., Kundu, C., Modem, S., Dubey, A., Flanagan, M.F.: Transmitter selection for secrecy in a frequency selective fading channel with unreliable Backhaul. IEEE 93rd Vehicular Technology Conference (VTC2021-Spring) (2021)
5. Wafai, B., Kundu, C., Dubey, A., Zhang, J., Flanagan, M.F.: Transmitter selection for secrecy in cognitive small-cell networks with Backhaul knowledge. IEEE 93rd Vehicular Technology Conference (VTC2021-Spring) (2021)
6. Yin, C., Garcia-Palacios, E.: Performance analysis for secure cooperative systems under unreliable backhaul over Nakagami-m channels. Mobile Networks and Appl. **24**, pp. 480-490 (2018)
7. Yin, C., Garcia-Palacios, E., Vo, N.-S., Duong, T.Q.: Cognitive heterogeneous networks with multiple primary users and unreliable backhaul connections. IEEE Access **7**, 3644–3655 (2019)
8. 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)
9. Li, X., Huang, M., Li, J., Yu, Q., Rabie, K., Cavalcante, C.C.: Secure analysis of multi-antenna cooperative networks with residual transceiver HIs and CEEs. IET Commun. **13**(17), 2649–2659 (2019)
10. Yin, C., Cheng, X., Li, Y., Liu, H.: Impact of wireless backhaul and imperfect channel estimation on secure communication networks. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 231–240 (2022)
11. Elsawy, H., Hossain, E., Kim, D.: HetNets with cognitive small cells: user offloading and distributed channel access techniques. IEEE Commun. Mag. **51**(6), 28–36 (2013)
12. ElSawy, H., Hossain, E.: Two-Tier hetnets with cognitive femtocells: downlink performance modeling and analysis in a multichannel environment. IEEE Trans. Mob. Comput. **13**(3), 649–663 (2014)

13. 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)
14. Nakagami, M.: The m-distribution—a general formula of intensity distribution of rapid fading. ScienceDirect (1960)