CoMP Transmission for Safeguarding Dense Heterogeneous Networks with Imperfect CSI

XU Yunjia, HUANG Kaizhi*, HU Xin, ZOU Yi, CHEN Yajun and JIANG Wenyu
National Digital Switching System Engineering & Technological Research Center
Zhengzhou, 450002 - CHINA
[e-mail: 136564061@qq.com]
*Corresponding author: HUANG Kaizhi

Received April 22, 2018; revised May 28, 2018; accepted June 5, 2018; published January 31, 2019

Abstract

To ensure reliable and secure communication in heterogeneous cellular network (HCN) with imperfect channel state information (CSI), we proposed a coordinated multipoint (CoMP) transmission scheme based on dual-threshold optimization, in which only base stations (BSs) with good channel conditions are selected for transmission. First, we present a candidate BSs formation policy to increase access efficiency, which provides a candidate region of serving BSs. Then, we design a CoMP networking strategy to select serving BSs from the set of candidate BSs, which degrades the influence of channel estimation errors and guarantees qualities of communication links. Finally, we analyze the performance of the proposed scheme, and present a dual-threshold optimization model to further support the performance. Numerical results are presented to verify our theoretical analysis, which draw a conclusion that the CoMP transmission scheme can ensure reliable and secure communication in dense HCNs with imperfect CSI.

Keywords: Dense heterogeneous cellular networks, imperfect CSI, physical layer security, CoMP transmission

This work has been partly supported by the National Natural Science Foundation of China under Grant No.61401510 and 61521003.

http://doi.org/10.3837/tiis.2019.01.007 **ISSN : 1976-7277**

1. Introduction

The wireless industry is currently facing an unprecedented growth of media business in the fifth generation (5G) mobile communication systems. For the purpose of capacity promotion, dense heterogeneous cellular network (HCN) has been regarded as a promising approach in 5G mobile communication systems [1, 2]. Nevertheless, due to the open architecture of interworking and broadcast nature of wireless communication, HCNs are intrinsically non-secure where information is easily detected and intercepted by malicious nodes (eavesdroppers). Traditionally, wireless security is guaranteed with high layer encryption, which faces difficulties of key distribution and computational complexity in dense HCNs. Secure communication is a crucial issue in HCNs. Thanks to physical layer security (PLS) enlightened by information theory, we can exploit differences between legitimate channel and wiretap channel to guarantee secure communication even without encryption. During the past decades, a framework of using PLS to ensure secure communication in dense HCNs has been developed in [3], and security performance without considering interference has been promoted in [4]. On this basis, researchers have designed many methods such as multiple-input multiple-output (MIMO) [5], secrecy beamforming [6], artificial noise (AN) [7], cooperative transmission [8], cooperative jamming [9] and resource allocation [10-12] to improve the security performance of wireless systems.

1.1 Related works and motivation

Most of the previous literature [3-12] is based on the hypothesis of perfect channel state information (CSI). While in practice, CSI is difficult to be perfectly known at each base station (BS) due to the channel estimation and quantization errors. [13] has investigated resource allocation under incomplete information between nodes in a randomly deployed D2D network, and has provided a game-theoretic mechanism to ensure reliable communication, which provides an effective idea for suppressing interference in D2D systems. To guarantee reliable and secure communication, Wang et al have analyzed the impact of artificial noise and have presented an optimal power allocation scheme for AN in multiple antennas system by a stochastic geometry approach [14, 15]. As nodes with single antenna cannot take advantage of the redundancy of multiple antennas, the proposed AN-aided transmission scheme cannot be used in the network where communication nodes are equipped with single antenna. In point-to-point communication network, Mu et al have put forward a secure On-Off transmission scheme to reduce the influence of channel estimation errors [16, 17]. However, the proposed scheme only considers channel estimation errors in a fixed communication link, which ignores the multi-link channel estimation errors caused by open access mechanism in dense HCNs. Additionally, robust beamforming [18], AN-assisted transmission scheme [19] and resource allocation [20] have been exploited in point-to-point communication network, but they neglect the random topology of dense HCNs. In cooperative transmission network, Chen et al have explored a CSI exchange scheme in multi-cell multi-input single-output (MISO) downlinks to improve the accuracy of CSI estimation and improve the security performance [21], while the cost of CSI exchanges increases with the number of communication nodes deploying in dense HCNs. In relay-aided networks, robust beamforming [22] and AN-aided transmission scheme [23] have been explored to improve the security performance. Inspired by these works, cooperative jamming [24] and relay/jammer selection scheme [25] have been proposed. Nevertheless, all of the aforementioned works

[16–25] only concentrate on networks with single access mechanism and fixed location and number of communication nodes, which cannot be applied to dense HCNs with random topology and multi-link channel estimation errors.

Furthermore, the dense deployment of communication nodes leads to complex interference, which results in pilot contamination and worse channel estimation. In order to diminish the additional inter-cell interference caused by such deployments, coordinated multipoint (CoMP) techniques have been introduced [26], where BSs communicate with each other over a backhaul link to limit the inter-cell interference and exploit the benefits of distributed multiple antenna systems [27, 28]. Besides, CoMP techniques also benefit security performance of HCNs effectively [29]. In summary, it is reasonable to consider reducing the interference and enhancing reliable and secure transmission at the same time. However, there still exist some challenges in the way of achieving reliable and secure communication in dense HCNs with imperfect CSI, which can be generalized as follows:

1) The random deployment and open access mechanism of dense HCNs result in irregular location and number of communication nodes. Therefore, the transmission schemes designed for fixed communication links are difficult to apply to networks with dynamic topologies.

2) In dense HCNs, multi-link channel estimation errors should be considered due to the open access mechanism, hence transmission schemes considering a fixed link with channel estimation error are inapplicable to dense HCNs.

3) Complex interference caused by dense deployment of communication nodes may lead to pilot contamination and poor channel estimation. Accordingly, how to decrease interference should be considered simultaneously in the transmission design.

1.2 Our work and contributions

Motivated by above observations and challenges, we introduce CoMP technology to guarantee reliable and secure communication, which has not been investigated for the PLS purpose in dense HetNets with imperfect CSI to the best of authors' knowledge. In this paper, we propose a CoMP transmission scheme based on dual-threshold optimization to improve the performance of dense HCNs, and provide a comprehensive performance analysis under a stochastic geometry framework, where the positions of BSs, users and eavesdroppers are all modeled as independent homogeneous Poisson Point Processes (PPPs). Our main contributions are summarized as follows:

1) A candidate BSs formation policy based on average received signal power (ARSP) is proposed to increase access efficiency. By setting access threshold, BSs with bad communication link qualities are prevented from being chosen as candidate BSs, and access efficiency has been greatly increased. On this basis, a CoMP networking strategy based on instantaneous estimated signal power (IESP) is presented. By setting networking threshold, only BSs with good channel conditions are able to serve the legitimate user, which guarantees reliable and secure communication.

2) Analyses of performance metrics including average achievable rate, connection outage probability (COP) and secrecy outage probability (SOP) are conducted for the proposed scheme in the presence of co-channel interference and the most detrimental eavesdroppers.

3) To further support the performance of the network, we present a dual-threshold optimization model, which maximizes the secrecy throughput subject to the security and reliability requirements of the network. Besides, we introduce a two-dimensional search method to obtain the optimal thresholds.

This paper is organized as follows. Section 2 introduces the system model in dense HCNs with channel estimation errors. Section 3 presents the CoMP transmission scheme based on

dual-threshold optimization. Section 4 explores the proposed approach by analyzing average achievable rate, COP and SOP. Simulation results and analysis are presented in Section 5. Section 6 concludes this paper.

Notations: We use $\mathcal{CN}\left(\mu,\sigma^2\right)$ to denote the noise following a circularly symmetric complex Gaussian with mean μ and covariance σ^2. $|\cdot|$, $\mathbb{P}(\cdot)$, and $\mathbb{E}(\cdot)$ denote absolute value, probability, and expectation, respectively. $F_A(\cdot)$ is the distribution function of a random variable A. $\exp(\lambda)$ represents exponential distribution with parameter λ. $f_A(\cdot)$ denotes probability density function (PDF) of A. $\mathcal{L}_A(\cdot)$ stands for the Laplace transform with respect to A. $Card(\cdot)$ represents the number of the entries in the input set.

2. System Model

2.1 Channel model

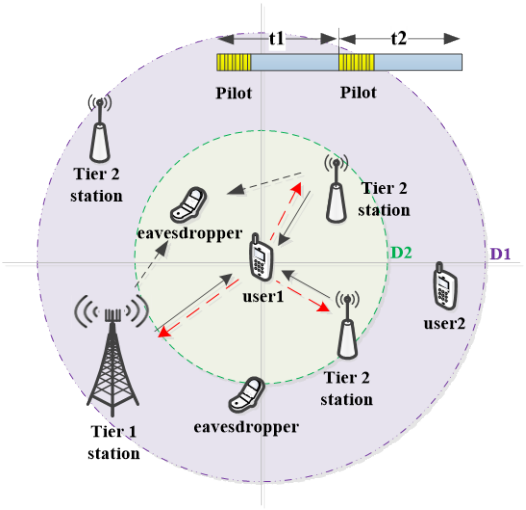

Fig. 1. A 2-tier dense HCN with CoMP transmission scheme

We consider dense HCNs composed of *K* independent network tiers of BSs (**Fig. 1** shows a 2-tier dense HCN). The BSs in the *i*-th tier are assumed to be with the same transmit power P_i. With respect to the random topology nature, the spatial positions of BSs are modeled as homogeneous PPP Φ_i with density λ_i.

We consider large scale and small scale fading at the same time. For the large scale fading model, we consider the standard path loss model, and the pass loss coefficient of the *i*-th tier is α_i, $\alpha_i > 2$. For the small scale fading, we adopt the independent quasi-static Rayleigh fading model and their channel gains follow the exponential distribution with unit mean.

Assuming the typical user is located at the origin without loss of generality. We denote a set of cooperating BSs by $\Upsilon \in \bigcup_{i=1}^{K} \Phi_i$, in which BSs cooperate to serve the typical user. Υ^c is the set of BSs out of Υ. The received signals at the typical user can be written as:

$$\sum_{B_{i,t}\in\Upsilon} \sqrt{P_i}\left|X_{i,t}\right|^{-\frac{\alpha_i}{2}} h_{i,t}s + \sum_{B_{l,u}\in\Upsilon^c} \sqrt{P_l}\left|Z_{l,u}\right|^{-\frac{\alpha_l}{2}} h_{l,u}s_x + Q \tag{1}$$

where $B_{i,t}$ is the *t*-th serving BS of the *i*-th tier in Υ, and $B_{l,u}$ is the *u*-th BS of the *l*-th tier in Υ^c. $X_{i,t}$ and $Z_{l,u}$ are the distance from $B_{i,t}$ and $B_{l,u}$ to the typical user, respectively. s and s_x are signals transmitted by serving BSs and non-serving BSs. $\sum_{B_{i,t}\in\Upsilon}\sqrt{P_i}\left|X_{i,t}\right|^{-\frac{\alpha_i}{2}}h_{i,t}s$ is the desired signal from Υ, and $\sum_{B_{l,u}\in\Upsilon^c}\sqrt{P_l}\left|Z_{l,u}\right|^{-\frac{\alpha_l}{2}}h_{l,u}s_x$ is the interference from Υ^c. Q is a standard additive circular symmetric complex white Gaussian random variable with variance σ^2.

2.2 Non-ideal channel estimation

In channel estimation phase, BSs transmit the pilot signals at each time slot. Users utilize the received pilot signals to estimate the current channels, and feed the estimated value back to BSs through ideal backhaul links. Since non-orthogonal pilots should be utilized among the cells with universal frequency reuse, the inter-cell interference causes pilot contamination, which results in imperfect CSI estimation. Without loss of generality, we assume BSs use the minimum mean square error (MMSE) estimation [30], the channel of $B_{i,t}$ is defined as:

$$h_{i,t}=\tilde{h}_{i,t}+o_{i,t} \tag{2}$$

where $h_{i,t}$ is the small scale fading coefficient of legitimate link, and $\tilde{h}_{i,t}$ is the estimated value of $h_{i,t}$. $o_{i,t}$ is the channel estimation error, $o_{i,t}\sim\mathcal{CN}\left(0,1-\rho_i\right)$, where $1-\rho_i$ is variance of $o_{i,t}$. We can consider $\rho_i\left(0\le\rho_i\le1\right)$ as channel estimation accuracy, and the high value of ρ_i indicates accurate channel estimation.

According to Slivnyak theorem, we consider a typical user accessing to $B_{i,t}$, the estimated SINR can be expressed as:

$$SINR_u^{\Theta}=\frac{\left|\sum_{B_{i,t}\in\Upsilon}\sqrt{P_i}\left|X_{i,t}\right|^{-\frac{\alpha_i}{2}}\tilde{h}_{i,t}\right|^2}{\sum_{B_{l,u}\in\Upsilon^c}P_l\left|Z_{l,u}\right|^{-\alpha_l}\left|\tilde{h}_{l,u}\right|^2+{\sigma_u}^2} \tag{3}$$

where $\sum_{B_{l,u}\in\Upsilon^c}P_l\left|Z_{l,u}\right|^{-\alpha_l}\left|\tilde{h}_{l,u}\right|^2$ is the received interference caused by non-serving BSs. $\tilde{h}_{l,u}$ is the estimated value of interference channel coefficient. ${\sigma_u}^2$ is the power of white Gaussian noise at the intended user.

Due to the impact of the channel estimation errors, the user's real received SINR can be expressed as:

$$SINR_u=\frac{\left|\sum_{B_{i,t}\in\Upsilon}\sqrt{P_i}\left|X_{i,t}\right|^{-\frac{\alpha_i}{2}}\tilde{h}_{i,t}\right|^2}{\sum_{B_{i,t}\in\Upsilon}P_i\left|X_{i,t}\right|^{-\alpha_i}\left|o_{i,t}\right|^2+\sum_{B_{l,u}\in\Upsilon^c}P_l\left|Z_{l,u}\right|^{-\alpha_l}\left|\tilde{h}_{l,u}\right|^2+\sum_{B_{l,u}\in\Upsilon^c}P_l\left|Z_{l,u}\right|^{-\alpha_l}\left|o_{l,u}\right|^2+{\sigma_u}^2} \tag{4}$$

where $\sum_{B_{i,t}\in\Upsilon}P_i\left|X_{i,t}\right|^{-\alpha_i}\left|o_{i,t}\right|^2$ and $\sum_{B_{l,u}\in\Upsilon^c}P_l\left|Z_{l,u}\right|^{-\alpha_l}\left|o_{l,u}\right|^2$ are the received interferences caused by the channel estimation errors.

Since the eavesdroppers wiretap the system passively, their instantaneous CSI and locations are unavailable. Nevertheless, we assume their small-scale channel distributions are available, which are Rayleigh fading with unit variance. Since only the legitimate user is identifiable to the network and can obtain CoMP transmission, we suppose non-colluding eavesdroppers estimate the channel accurately, operating in open single access mode, i.e., access to only one of the BSs in Υ to wiretap. Considering the worst case, the receive SINR at the most malicious eavesdropper is given by:

$$SINR_e = \max_{e\in\Phi_e}\left\{\frac{P_i\left|Y_{i,e}\right|^{-\alpha_i}\left|h_{i,e}\right|^2}{\sum_{B_{l,u}\in\Upsilon^c}P_l\left|L_{l,e}\right|^{-\alpha_l}\left|h_{l,e}\right|^2+\sigma_e^{\ 2}}\right\} \tag{5}$$

where $Y_{i,e}$ is the distance from the serving BS $B_{i,t}$ to the eavesdropper, and $h_{i,e}$ is the coefficient of wiretap channel. $\sum_{B_{l,u}\in\Upsilon^c}P_l\left|L_{l,e}\right|^{-\alpha_l}\left|h_{l,e}\right|^2$ is the interference received by the eavesdropper, where $h_{l,u}$ is the coefficient of interference channel, and $L_{l,e}$ is the distance from the interference BS $B_{l,u}$ to the eavesdropper. $\sigma_e^{\ 2}$ is the power of white Gaussian noise received by the eavesdropper.

3. CoMP Transmission Scheme

In this section, we design a CoMP transmission scheme based on dual-threshold optimization in dense HCNs with imperfect CSI. First, we propose an ARSP based candidate BSs formation policy to increase access efficiency. Then, we design a CoMP networking strategy based on IESP to select serving BSs from the set of candidate BSs, which declines the influence of channel estimation errors. By the dual-threshold based CoMP transmission scheme, only BSs with good communication link qualities are selected for transmission, which guarantees reliable and secure communication.

3.1 Candidate BSs formation policy

In an open-access system, users are served by BSs from arbitrary tiers, which lower the access efficiency of the network. To increase access efficiency effectively, an ARSP based candidate BSs formation policy is proposed, which avoids users accessing BSs with bad channel conditions. In this policy, an access threshold τ is introduced, where BSs are opted to the cluster of candidate BSs only if users received ARSPs are larger than τ. Mathematically, the proposed candidate BSs formation policy is expressed as:

$$P_i\left|X_{i,t}\right|^{-\alpha_i} > \tau \tag{6}$$

Specifically, it can be deduced that users can access BSs when the distance $X_{i,t}$ from the user to the BS is closer than D_i, where $D_i = \left(P_i/\tau\right)^{1/\alpha_i}$ denotes the radius of the candidate region in the *i*-th tier. In other words, all the candidate BSs should be located inside a circular area, i.e., $X_{i,t}\in\left(0, D_i\right]$.

Based on the proposed candidate BSs formation policy, the candidate region of BSs in each tier has been clearly shown in **Fig. 1**. Due to different operating parameters, the candidate regions for each tier are different. Since the locations of BSs are distributed as uniform PPPs,

the distance $X_{i,t}$ between $B_{i,t}$ and the typical user is uniform distribution over the circular area with the radius D_i. Hence, the PDF of $X_{i,t}$ is:

$$f_{X_{i,t}}\left(x_{i,t}\right)=\frac{2x_{i,t}}{D_i^2},\ 0<x_{i,t}<D_i \tag{7}$$

According to the property of PPPs, the number of candidate BSs in the *i*-th tier is:

$$M_i=\lambda_i\pi D_i^2 \tag{8}$$

It is worth mentioning that the candidate BSs formation policy benefits the system performance in the following three aspects:

1) It restrains the legitimate user from associating with BSs outside the candidate region, such that not only a good communication link quality can be guaranteed but also complex interference can be abstained. Therefore, the qualities of communication links are improved consequently, which has the potential of increasing reliability performance.

2) Since ARSP of BS outside the serving region is always inferior to that inside, the policy can help to avoid eavesdroppers wiretapping messages out of the candidate region. Therefore, security performance can be guaranteed.

3) BSs are allowed to be selected in the candidate region of each tier, which greatly increases the efficiency of CoMP BSs selection in *K*-tier dense HCNs.

It is worth mentioning that the proposed CoMP transmission scheme based on dual-threshold optimization is different from conventional CoMP transmission scheme [26]. Our proposed transmission scheme takes channel estimation errors into account, and only BSs with good communication link qualities are allowed for CoMP transmission, which benefits reliable and secure transmission in the system with channel estimation errors.

3.2 CoMP networking strategy

To select BSs with good communication link qualities, an IESP based CoMP networking strategy has been designed, which avoids BSs with poor channel conditions serving the legitimate user. In this policy, a networking threshold θ is introduced, where BSs in the candidate region are selected as serving BSs only when users received IESPs are larger than θ. Mathematically, the CoMP networking strategy is expressed as:

$$\left|\sqrt{P_i}\left|X_{i,t}\right|^{-\frac{\alpha_i}{2}}\tilde{h}_{i,t}\right|^2>\theta \tag{9}$$

Customarily, θ should be decreased sensibly when there exist less channel estimation errors in the current communication links. Therefore, the preponderance of CoMP transmission can be fully used. Otherwise, θ should be increased when the current channels are in poor conditions. Hence, only BSs with good communication link qualities are chosen as serving BSs by adjusting θ according to the current channel status and the user requirements.

The probability of $B_{i,t}$ being chosen as serving BS is given by:

$$P_c^{i,t}=\mathbb{P}\left\{\left|\tilde{h}_{i,t}\right|^2>\frac{\theta}{P_i\left|X_{i,t}\right|^{-\alpha_i}}\right\}=\frac{1}{\rho_i}\exp\left(-\frac{\theta}{\rho_i P_i\left|X_{i,t}\right|^{-\alpha_i}}\right) \tag{10}$$

The probability of N_i BSs participating in CoMP transmission in the *i*-th tier can be expressed as:

$$\mathbb{P}\left(N_i=n_i\right)=\mathrm{C}_{M_i}^{n_i}\left(P_c^{i,t}\right)^{n_i}\left(1-P_c^{i,t}\right)^{M_i-n_i} \tag{11}$$

Denote $\boldsymbol{X}_i = \left[X_{i,1}, X_{i,2}, \cdots, X_{i,N_i} \right]$ as the distance vector of the i-th tier. Due to the independence of $X_{i,t}\left(t = 1, \cdots, N_i\right)$, the joint PDF of elements in $\boldsymbol{X}_i$ is characterized as:

$$f_{\boldsymbol{X}_i} = 2^{N_i} \prod_{t=1}^{N_i} x_{i,t} \Big/ D_i^{2N_i}, \ 0 \le x_{i,t} \le D_i \tag{12}$$

In the following sections, we provide a comprehensive analysis of the proposed approach in dense HCNs incorporating average achievable rate, COP and SOP, respectively. By deriving various analytical expressions of our performance metrics, we aim to provide tractable predictions of network performance and guidelines for future network designs.

4. Performance Analysis and Optimization

4.1 Average achievable rate

In this subsection, we introduce the approach of analyzing average achievable rate, which is an important metric to measure the capacity of a communication link. In the proposed scheme, the average achievable rate R_u is determined by the number of serving BSs. We define $R_u^{\{n_1,n_2,\cdots,n_K\}} = \mathbb{E}\left\{\log_2\left(1+\left(1/SINR_u^{\{n_1,n_2,\cdots,n_K\}}\right)\right)\right\}$ as the average achievable rate with $\sum_{i=1}^{K} N_i$ serving BSs. Employing the total probability formula, the average achievable rate can be expressed as:

$$R_u = \sum_{n_1=1}^{M_1} \cdots \sum_{n_K=1}^{M_K} \prod_{i=1}^{K} \mathbb{P}\left(N_i = n_i\right) R_u^{\{n_1,n_2,\cdots,n_K\}} \tag{13}$$

We solve $R_u^{\{n_1,n_2,\cdots,n_K\}}$ to obtain the accurate expression of R_u. Since it is difficult to have the accurate expression of $R_u^{\{n_1,n_2,\cdots,n_K\}}$, we consider the lower bound of average achievable rate with $\sum_{i=1}^{K} N_i$ serving BSs, noted as $R_u^{L|\{n_1,n_2,\cdots,n_K\}}$. According to Jensen inequality, we can obtain:

$$R_u^{L|\{n_1,n_2,\cdots,n_K\}} \triangleq \log_2\left(1+\left[\mathbb{E}\left(1/SINR_u^{\{n_1,n_2,\cdots,n_K\}}\right)\right]^{-1}\right) \le \mathbb{E}\left\{\log_2\left(1+\left(1/SINR_u^{\{n_1,n_2,\cdots,n_K\}}\right)\right)\right\} \tag{14}$$

Theorem 1 The lower bound of average achievable rate with channel estimation errors is:

$$R_u^{L} = \sum_{n_1=1}^{M_1} \cdots \sum_{n_K=1}^{M_K} \prod_{i=1}^{K} \mathrm{C}_{M_i}^{n_i} \left(P_c^{i,t}\right)^{n_i} \left(1-P_c^{i,t}\right)^{M_i-n_i} R_u^{L|\{n_1,n_2,\cdots,n_K\}} \tag{15}$$

where

$$R_u^{L|\{n_1,n_2,\cdots,n_K\}} = \log_2\left(1+\frac{\sum_{i=1}^{K} \frac{2P_i n_i}{D_i^2 \rho_i\left(\alpha_i-2\right)}}{\sum_{i=1}^{K} \frac{2P_i}{D_i^2\left(1-\rho_i\right)\left(\alpha_i-2\right)} + \sum_{l=1}^{K} \frac{2P_l\left[\rho_l+\pi\lambda_l\left(1-\rho_l\right)\right]}{D_l^2\left(1-\rho_l\right)\rho_l\left(\alpha_l-2\right)} + {\sigma_u}^2}\right) \tag{16}$$

Proof: See Appendix A.

Note that the dual thresholds of the proposed scheme can both influence average achievable rate according to (15) and (16). We show the effects of access threshold τ on average achievable rate, COP and SOP in **Fig. 2**. It is obvious that the average achievable rate increases with τ first, and then decreases. As τ determines the number of candidate BSs, a lower τ implies a wider candidate region and a bigger cluster of candidate BSs. Especially, $\tau = 0$ means that the system is without the candidate BSs formation policy. BSs in bad conditions

may be selected as candidate BSs, and the interference from those BSs may lower the received SINR of legitimate user. The increase of τ provides the ambit that only BSs with good communication link qualities have chances to serve the legitimate user, hence the average achievable rate increases. With further increase of τ, fewer BSs in the network can achieve the requirement where users received ARSPs are larger than τ, hence the average achievable rate drops. As a result, there exists an optimal τ to achieve the maximum average achievable rate.

Another important parameter is the networking threshold θ, which affects not only the quality but also the number of serving BSs according to (10) and (11). We show the effects of networking threshold θ on average achievable rate, COP and SOP in **Fig. 3**. It is obvious that the average achievable rate is not a monotonic function of θ, which increases first and decreases later with the increase of θ. Particularly, $\theta = 0$ means that any BSs in the candidate region can serve the legitimate user. However, not all the BSs in the candidate region are in good channel conditions, and the average achievable rate is in a low level. The initial increase of θ provides the limit that only BSs with good communication link qualities can be selected as serving BSs, hence the average achievable rate increases. With further increase of θ, fewer BSs can be chosen as serving BSs, and the average achievable rate diminishes. Therefore, there exists an optimal θ to achieve the maximum average achievable rate.

4.2 COP

COP is an important metric to measure the reliability of communication link. If the capacity of legitimate channel is less than the transmission rate, there will be a connection outage event. For a given transmission rate R_b, COP of the typical user is expressed as [17]:

$$P_{co} = \mathbb{P}\left(\log_2\left(1+SINR_u\right) \le R_b\right) \tag{17}$$

To obtain the expression of P_{co}, (17) can be transformed into $P_{co} = 1-\mathbb{P}\left(\log_2\left(1+SINR_u\right) > R_b\right)$. We define $P_c^{\{n_1,n_2,\cdots,n_K\}} = \mathbb{P}\left(\log_2\left(1+SINR_u^{\{n_1,n_2,\cdots,n_K\}}\right) > R_b\right)$ as the coverage probability of $\sum_{i=1}^{K} N_i$ serving BSs, which can be given by:

$$P_c^{\{n_1,n_2,\cdots,n_K\}} = \mathbb{E}_{X_{i,t}}\left\{\mathbb{P}\left(\frac{\left|\sum_{i=1}^{K}\sum_{t=1}^{N_i}\sqrt{P_i}\left|X_{i,t}\right|^{-\frac{\alpha_i}{2}}\tilde{h}_{i,t}\right|^2}{I_{io}+I_{IS}+I_{lo}+\sigma_u^2} > \gamma\right)\right\} \tag{18}$$

where $\gamma = 2^{R_b}-1$, $I_{io} = \sum_{B_{i,t}\in\Upsilon} P_i\left|X_{i,t}\right|^{-\alpha_i}\left|o_{i,t}\right|^2$ and $I_{lo} = \sum_{B_{l,u}\in\Upsilon^c} P_l\left|Z_{l,u}\right|^{-\alpha_l}\left|o_{l,u}\right|^2$ are the cumulative interferences caused by channel estimation errors from the serving BSs and non-serving BSs, respectively. $I_{lS} = \sum_{B_{l,u}\in\Upsilon^c} P_l\left|Z_{l,u}\right|^{-\alpha_l}\left|\tilde{h}_{l,u}\right|^2$ is the received interference caused by non-serving BSs at the intended user.

Employing the total probability formula, P_{co} can be expressed as:

$$P_{co} = 1-\sum_{n_1=1}^{M_1}\cdots\sum_{n_K=1}^{M_K}\prod_{i=1}^{K}\mathbb{P}\left(N_i = n_i\right)P_c^{\{n_1,n_2,\cdots,n_K\}} \tag{19}$$

By solving $P_c^{\{n_1,n_2,\cdots,n_K\}}$, we can obtain the accurate expression COP as shown in Theorem 2.

Theorem 2 The COP of the typical legitimate user is:

$$P_{co}=1-\sum_{n_1=1}^{M_1}\cdots\sum_{n_K=1}^{M_K}\prod_{i=1}^{K}\mathbb{P}\left(N_i=n_i\right)\underbrace{\int\cdots}_{\boldsymbol{x}_1,\cdots,\boldsymbol{x}_K}\int\Xi\exp\left(-\frac{\gamma\sigma_u^2}{\chi}\right)d\boldsymbol{x}_1,\cdots,d\boldsymbol{x}_K \tag{20}$$

where $\chi=\sum_{i=1}^{K}\sum_{t=1}^{N_i}\rho_i P_i\left|x_{i,t}\right|^{-\alpha_i}$, $\Xi=\prod_{i=1}^{K}\frac{1}{\rho_i}\mathcal{L}_{I_{io}}\left(\frac{\gamma}{\chi}\right)\prod_{l=1}^{K}\mathcal{L}_{I_{ls}}\left(\frac{\gamma}{\chi}\right)\mathcal{L}_{I_{lo}}\left(\frac{\gamma}{\chi}\right)f_{\boldsymbol{x}_i}(x)$. When $\alpha_i=\alpha_l=\alpha$, $\mathcal{L}_{I_{io}}\left(\gamma\chi^{-1}\right)=\exp\left\{-\pi\lambda_i\psi\left(\left(1-\rho_i\right)\gamma P_i\chi^{-1}\right)^{2/\alpha}\right\}$, $\mathcal{L}_{I_{ls}}\left(\gamma\chi^{-1}\right)=\exp\left\{-\pi\lambda_i\psi\left(\rho_l\gamma P_l\chi^{-1}\right)^{2/\alpha}\right\}$, $\mathcal{L}_{I_{lo}}\left(\gamma\chi^{-1}\right)=\exp\left\{-\pi\lambda_i\psi\left(\left(1-\rho_l\right)\gamma P_l\chi^{-1}\right)^{2/\alpha}\right\}$, where $\psi=\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)$.

Proof: See Appendix B.

As COP reflects the relationship between average achievable rate and the given outage threshold, for a given threshold R_b, COP is a decreasing function of R_u. The changing trend of COP is opposite to R_u. COP decreases with τ first, and then increases in **Fig. 2**. Particularly, $\tau=0$ indicates that arbitrary BSs in the system have chance to serve the legitimate user. BSs with poor communication link qualities may affect the reliability of the system, and COP is at a high level at the beginning. As τ limits the link qualities of candidate BSs, the increase of τ enhances the reliability of network, and COP decreases. With further increase of τ, fewer BSs in the network can be selected as candidate BSs, and COP increases. Accordingly, there exists an optimal τ to achieve the minimum COP.

We can see that COP decreases first and increases later with the increase of θ in **Fig. 3**. Especially, $\theta=0$ specifies that there is no CoMP networking strategy in the system. It means that any BSs in the candidate region can serve the legitimate user. Interference from BSs with channel estimation errors may reduce the reliability of the system, which leads to a high COP. Since θ affects not only the quality but also the number of serving BSs, the initial increase of θ enhances the qualities of communication links by selecting BSs with good channel conditions, hence COP declines. With further increase of θ, less BSs can achieve the demand where users received IESPs are larger than θ, and COP increases. Therefore, we can search an optimal θ to achieve the minimum COP.

4.3 SOP

Secrecy outage probability is the principle performance metric in the passive eavesdropping scenario. The secrecy outage is declared when the instantaneous secrecy rate is less than the targeted secrecy rate. For a given confidential rate R_s, the SOP of the intended user is given by [17]:

$$P_{so}=\Pr\left(\log_2\left(1+SINR_e\right)>R_u-R_s\right) \tag{21}$$

(21) can be transformed into $P_{so}=1-\mathbb{F}_{SINR_e}\left(2^{(R_u-R_s)}-1\right)$, where $\mathbb{F}_{SINR_e}(\cdot)$ is the distribution function of $SINR_e$.

Since eavesdroppers work in open single access mode, they access the BS providing maximal receiving power. The access probability of eavesdroppers associate in the BS of the *i*-th tier is given by [31]:

$$\mathcal{A}_i = 2\pi\lambda_i \int_0^{\infty} y \exp\{-\pi \sum_{j=1}^{K} \lambda_j (\frac{P_j}{P_i})^{2/\alpha_j} y^2\} dy \tag{22}$$

Employing the total probability formula, SOP is expressed as:

$$P_{so} = \sum_{i=1}^{K} \mathcal{A}_i \cdot P_{so}^i \tag{23}$$

where P_{so}^i denotes SOP in the *i*-th tier.

We consider the most dangerous scenario where transmission is secure only if secrecy rate is achieved against all eavesdroppers. When $\alpha_i = \alpha_l = \alpha$, SOP in the *i*-th tier can be derived as:

$$\begin{aligned} P_{so}^i &= \mathbb{P}\left\{ \max_{e \in \Phi_e} \left\{ \frac{P_i \left| Y_{i,e} \right|^{-\alpha} \left| h_{i,e} \right|^2}{I_{le} + \sigma_e^{\,2}} \right\} > \upsilon \right\} \\ &= 1 - \exp\left(-2\pi\lambda_e \int_{D_i}^{\infty} \mathbb{E}\left[\exp\left(-\frac{I_{le} + \sigma_e^{\,2}}{P_i y_{i,e}^{\ -\alpha}} \upsilon \right) \right] y_{i,e} dy_{i,e} \right) \\ &= 1 - \exp\left(-2\pi\lambda_e \int_{D_i}^{\infty} \prod_{l=1}^{K} \mathcal{L}_{I_{le}}\left(\frac{\upsilon}{P_i y_{i,e}^{\ -\alpha}} \right) \exp\left(-\frac{\sigma_e^{\,2}}{P_i y_{i,e}^{\ -\alpha}} \upsilon \right) y_{i,e} dy_{i,e} \right) \end{aligned} \tag{24}$$

where $\upsilon = 2^{R_u - R_s} - 1$, $I_{le} = \sum_{B_{l,u} \in \Upsilon^c} P_l \left| L_{l,e} \right|^{-\alpha_l} \left| h_{l,e} \right|^2$ is the received interference caused by non-serving BSs at the eavesdropper, and its Laplace transform can be expressed as:

$$\mathcal{L}_{I_{le}}\left(\frac{\upsilon}{P_i y_{i,e}^{\ -\alpha}} \right) = \exp\left\{ -\pi\lambda_l \Gamma\left(1 + \frac{2}{\alpha}\right) \Gamma\left(1 - \frac{2}{\alpha}\right) \left(\frac{\upsilon P_l}{P_i} \right)^{2/\alpha} y_{i,e}^{\ 2} \right\} \tag{25}$$

By plugging P_{so}^i into (23), we can obtain the expression of P_{so} as shown in theorem 3.

Theorem 3 The SOP of the intended user can be expressed as:

$$P_{so} = \sum_{i=1}^{K} \mathcal{A}_i \cdot \left\{ 1 - \exp\left(-2\pi\lambda_e \int_0^{\infty} \prod_{l=1}^{K} \exp\left\{ -\pi\lambda_l \psi \left(\frac{\upsilon P_l}{P_i} \right)^{2/\alpha} y_{i,e}^{\ 2} \right\} \exp\left(-\frac{\upsilon \sigma_e^{\,2}}{P_i y_{i,e}^{\ -\alpha}} \right) y_{i,e} dy_{i,e} \right) \right\} \tag{26}$$

In **Fig. 2**, we illustrate the relationship between SOP and τ. We observe that SOP decreases first and then increases as τ increases. It is because the number of eavesdroppers always increases with the increase of access threshold, which augments the capacity of wiretap channel. Thanks to the increase of τ, BSs satisfying the candidate qualification are selected as candidate BSs, which ameliorates the qualities of communication links. However, continuous increase of τ makes few BSs meet the candidate requirement, and the capacity of legitimate channel decreases. Therefore, the capacity of legitimate channel increases first but then decreases with the increase of τ. In summary, SOP declines first and increases later, as the security capacity is the difference between the capacity of the legitimate channel and wiretap channel.

We show the relationship between SOP and θ in **Fig. 3**. It is obvious that SOP decreases first and then increases with the increasing θ. This can be explained by the fact that when $\theta = 0$, arbitrary BSs in the candidate region are serving BSs. While BSs in the cellular cell edge reduce the capacity of legitimate channel, meanwhile improving the possibility of eavesdropping, SOP is at a high level at the beginning as a result. The initial increase of θ

enhances the qualities of communication links, which strengthens the capacity of legitimate channel and decreases the capacity of wiretap channel simultaneously, hence SOP declines. With further increase of θ, less BSs can serve the legitimate user, which leads to the capacity diminishment of legitimate channel and wiretap channel at the same time. Nevertheless, the capacity decline of legitimate channel is more pronounced, and SOP increases. Consequently, SOP decreases first and increases later with the increase of θ, and there exists an optimal θ to achieve the minimum SOP.

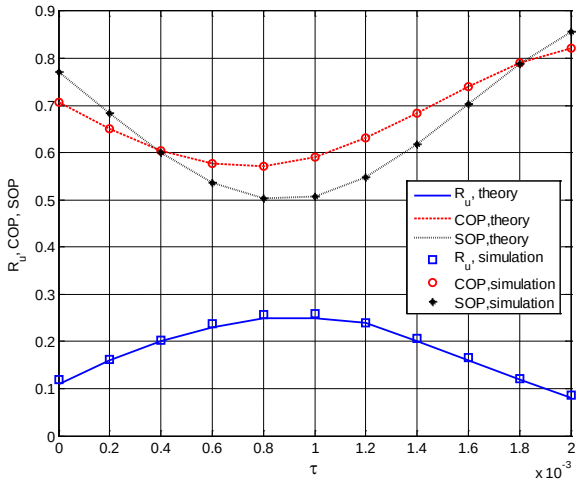

Fig. 2. Average achievable rate, COP and SOP versus access threshold

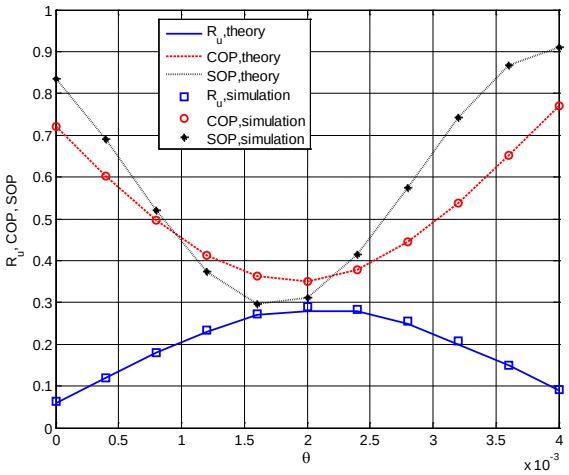

Fig. 3. Average achievable rate, COP and SOP versus networking threshold

4.4 Performance optimization

From the analyses of average achievable rate, COP and SOP, we verify the validity of the proposed scheme. As secrecy throughput measures security performance and reliability performance simultaneously, we consider secrecy throughput as the metric for performance optimization, which is defined as the average achievable rate that is reliably and securely transmitted from the transmitters to the intended receivers. Mathematically, the secrecy throughput is given by:

$$\xi = \left(1 - p_{co}\right)\left(1 - p_{so}\right) R_u \tag{27}$$

It is obvious that the dual thresholds, i.e., τ and θ, affect both the reliability and security of the system. The relationship between secrecy throughput and τ, θ are demonstrated in **Fig. 4**. As can be observed from the curves, the secrecy throughput increases first and then decreases with the increase of τ and θ. There exist optimal values τ^* and θ^* to achieve the maximum value of secrecy throughput. Therefore, it is significant to set appropriate dual thresholds to decrease the influence of channel estimation errors and guarantee reliable and secure communication. To further support the performance of the system, we present a dual-threshold optimization model, which maximizes the secrecy throughput subject to the security and reliability requirements of the network.

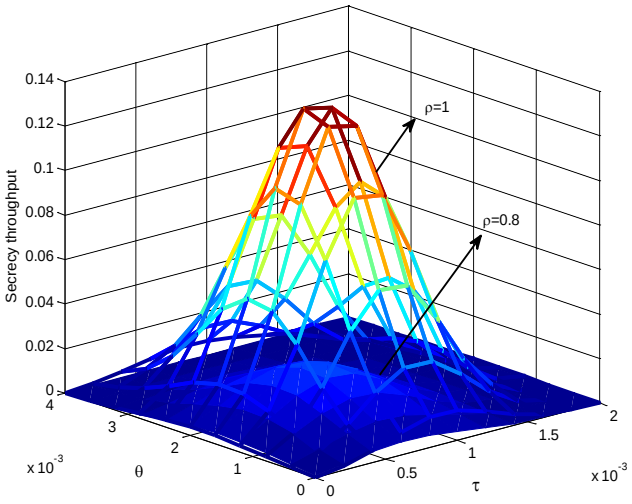

Fig. 4. Secrecy throughput versus τ and θ

In practice, BSs have the same communication requirements in different layers. The security constraints and reliable constraints can be defined as ε and δ respectively. The optimization problem aiming to maximize the secrecy throughput can be expressed as:

$$\begin{aligned} \max_{\tau,\theta} \quad & \xi = \left(1 - P_{co}\right)\left(1 - P_{so}\right) R_u, \\ s.t. \quad & C1: P_{so} \le \varepsilon, P_{co} \le \delta \\ & C2: \varepsilon \in [0,1], \delta \in [0,1] \\ & C3: \tau \in \left[0, \tau^{up}\right], \theta \in \left[0, \theta^{up}\right] \end{aligned} \tag{28}$$

where τ^{up} and θ^{up} denote the upper access threshold and networking threshold to satisfy reliable and secure communication.

As it is difficult to obtain the analytical results from (28), we employ a two-dimensional search method to get the optimal results of τ and θ. The feasible solutions $\left(\hat{\tau}, \hat{\theta}\right)$ are obtained by the constraint $C1$ in (28), which satisfies the security and reliability requirements of the network. The optimal values τ^* and θ^* to maximize the secrecy throughput should be those in the set $\left(\hat{\tau}, \hat{\theta}\right)$. Mathematically, we can get the optimal values τ^* and θ^* by:

$$\left(\tau^*, \theta^*\right) = \max_{\tau,\theta} \ \xi\left(\hat{\tau}, \hat{\theta}\right) \tag{29}$$

Based on the analysis above, we present a two-dimensional search method to numerically determine the optimal values τ^* and θ^* of the access threshold and networking threshold, respectively. As shown in **Table 1**, we respectively denote the step size of τ, θ as $\Delta\tau$, $\Delta\theta$.

Table 1. Two-dimensional search method for obtaining optimal values τ^* and θ^*

Algorithm 1

1: Input: K, $\rho_i(i=1,\cdots,K)$, $\alpha_i(i=1,\cdots,K)$, $P_i(i=1,\cdots,K)$, $\lambda_i(i=1,\cdots,K)$, λ_e, R_b, R_s, τ^{up}, θ^{up}, ε, δ, $\Delta\tau$, $\Delta\theta$;
2: Output: τ^*, θ^*;
3: Initialization: $C = \frac{\tau^{up}}{\Delta\tau}$, $V = \frac{\theta^{up}}{\Delta\theta}$, set $\xi^{temp} = 0$;
4: **for** $c = 1:C$ **do**
5: **for** $v = 1:V$ **do**
6: Calculate P_{co} in (20) and P_{so} in (26);
7: **if** $P_{co} \le \delta$ and $P_{so} \le \varepsilon$ **then**
8: update the set $\left(\hat{\tau}, \hat{\theta}\right)$ by putting $\Delta\tau \cdot c$, $\Delta\theta \cdot v$ into the set $\left(\hat{\tau}, \hat{\theta}\right)$;
9: **end if**
10: **end for**
11: **end for**
12: Set Ω as the number of entries in the determined set $\hat{\tau}$ and $\hat{\theta}$. That is $\Omega = Card\left(\hat{\tau}\right) = Card\left(\hat{\theta}\right)$;
13: **for** $\omega = 1:\Omega$ **do**
14: Calculate ξ by substituting the entries τ_ω, θ_ω into (27) that lie in the determined set $\left(\hat{\tau}, \hat{\theta}\right)$;
15: **if** $\xi > \xi^{temp}$ **then**
16: $\xi^{temp} = \xi$;
17: Update τ^*, θ^* by $\tau^* = \tau_\omega$, $\theta^* = \theta_\omega$;
18: **end if**
19: **end for**
20: Return τ^*, θ^*; (The optimal values are obtained.)

5. Numerical Results

In this section, we provide more detail simulation and numerical results to evaluate and analyze the performance of our proposed scheme. For simplicity, we consider a 2-tier dense HCN, in which macrocell base stations (MBSs) and picrocell base stations (PBSs) are deployed. We set the density of MBSs, PBSs and eavesdroppers as $\lambda_1 = 1/\pi 500^2\, m^2$, $\lambda_2 = 5\lambda_1$ and $\lambda_e = 5\lambda_1$, respectively. The transmission power and path fading coefficients are

$P_1 = 20W, P_2 = 2W, \alpha_1 = \alpha_2 = 4$. The confidential information rate is $R_s = 0.1$bit/s/Hz, and the access threshold and networking threshold are set according to algorithm 1. We adopt the PPP model on the network with radius $R_c = 500m$.

5.1 The effects of channel estimation accuracy

In **Fig. 5** and **Fig. 6**, we plot the COP and SOP versus channel estimation accuracy respectively to show the effects of channel estimation on reliability and security performances. We set $\rho = \rho_1 = \rho_2$ to illustrate the influence of channel estimation accuracy. As shown in the figure, the analytical results of COP and SOP are in quite good agreement with simulation results. It validates the accuracy of our analytical results. Observed that COP and SOP are decreasing functions of ρ. This implies that channel estimation errors influence the qualities of communication links, and less channel estimation errors (high ρ) can increase reliability and security of the system. It is evident that accurate channel estimation counts much in reliable and secure communication.

Comparing the curves of τ=0, θ=0 with $\tau \neq 0, \theta \neq 0$ in **Fig. 5** and **Fig. 6**, we can observe that the system without the proposed CoMP transmission scheme has the highest COP and SOP among those with the proposed scheme. The curves illustrate that the proposed scheme can decrease COP by at most 50% and decrease SOP by at most 65%, which verifies that the CoMP transmission scheme can improve reliability and security performances of the network effectively.

Comparing the curves of τ=0.001, θ=0.002, τ=0.001, θ=0 and τ=0, θ=0.002, we can see that COP and SOP of the system with the proposed scheme varies with the thresholds. Since τ=0.001, θ=0.002 is the optimal value of dual thresholds when $\rho = 1$ according to algorithm 1, the COP and SOP of the system with the optimal thresholds are reasonably lower than other results. This indicates that appropriate thresholds setting can enhance the reliability and security performances of the system efficaciously. Simultaneously, the validity of algorithm 1 is testified.

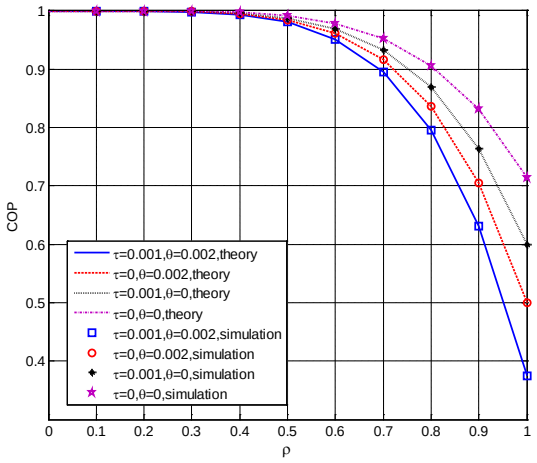

Fig. 5. COP versus channel estimation accuracy

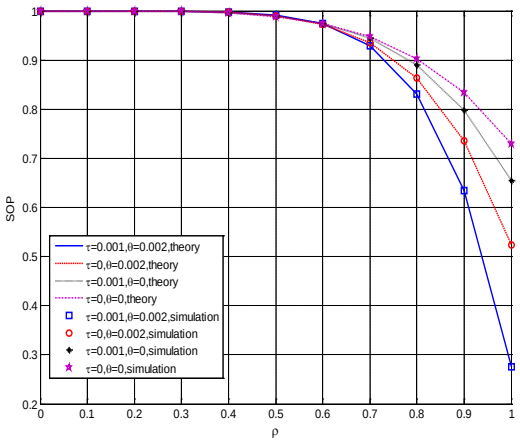

Fig. 6. SOP versus channel estimation accuracy

The average achievable rate and secrecy throughput of the legitimate user over different channel estimation accuracy are shown in **Fig. 7** and **Fig. 8**. Note that the average achievable rate and secrecy throughput monotonically increase with channel estimation accuracy. As accurate channel estimation ensures the qualities of communication links, high channel estimation accuracy can increase average achievable rate and secrecy throughput. It is of paramount significant to enhance the channel estimation accuracy.

Comparing the curves of τ=0, θ=0 with $\tau \neq 0, \theta \neq 0$ in **Fig. 7** and **Fig. 8**, we can find that the system without the proposed CoMP transmission scheme has the lowest average achievable rate and secrecy throughput among those with the proposed scheme. It can be seen that the proposed scheme can increase average achievable rate by at most 0.22 bit/s/Hz and increase secrecy throughput by at most 0.13 bit/s/Hz, which verifies that the CoMP transmission scheme can improve average achievable rate and secrecy throughput of the network effectively.

Comparing the curves of τ=0.001, θ=0.002 , τ=0.001, θ=0 and τ=0, θ=0.002 , we notice that the curves of τ=0.001, θ=0.002 are the highest among the others. As mentioned before, τ=0.001, θ=0.002 is the optimal value of dual thresholds when $\rho = 1$. The average achievable rate and secrecy throughput of the system with the optimal thresholds is reasonably higher than other results. This indicates that appropriate thresholds setting can enhance the average achievable rate and secrecy throughput of the system efficaciously.

The observations from **Fig. 5-8** indicate the validity of the proposed CoMP transmission scheme in improving the reliability and security performances of the system with imperfect CSI, and verify the effectiveness of the two-dimensional search method in algorithm 1 to obtain the optimal values of the dual thresholds. In addition, the above-mentioned results also validate that it is always significant to improve channel estimation accuracy to improve the performance of dense HCNs with imperfect CSI.

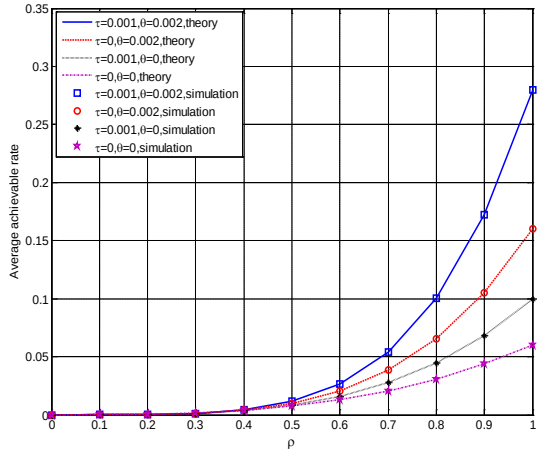

Fig. 7. Average achievable rate versus channel estimation accuracy

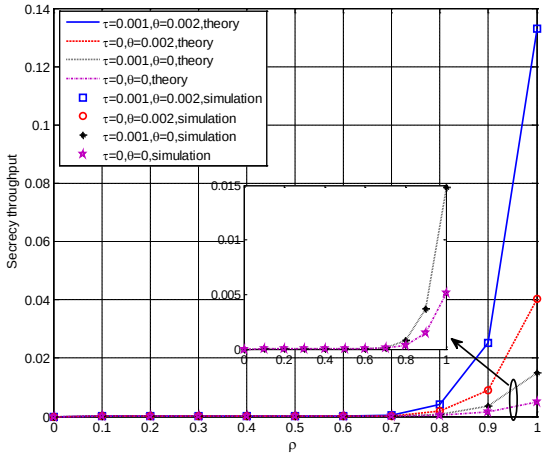

Fig. 8. Secrecy throughput versus channel estimation accuracy

5.2 The effects of eavesdroppers' density and PBSs' density

In this subsection, we plot the secrecy throughput versus eavesdroppers' density to show the influence of eavesdroppers' density and PBSs' density in **Fig. 9**. When deploying BSs in HCNs, the ability of channel estimation and deploying density of BSs may affect the system performance. Since MBSs and PBSs play similar parts in the system, we take PBSs as an example to discuss the influence of the BSs deploying in HCNs.

As can be seen from the curves in **Fig. 9**, the secrecy throughput decreases with the increase of eavesdroppers. Since the increase of eavesdroppers reduces the security performance, the secrecy throughput declines.

Comparing the curves of $\tau = 0, \theta = 0$ with $\tau = 0.001, \theta = 0.002$ when $\rho_2 = 1, \lambda_2 = 3\lambda_1$, we can see that the secrecy throughput of the system with the proposed scheme is higher than that without the proposed scheme, which verifies that the CoMP transmission scheme can improve secrecy throughput of the network effectively.

To illustrate the influence of deploying PBSs with the same channel estimation capacity, we compare the curves of $\lambda_2 = 3\lambda_1$ with $\lambda_2 = 5\lambda_1$ under the condition where PBSs can estimate the channel accurately and the system works with the proposed transmission scheme, i.e., $\rho_2 = 1, \tau = 0.001, \theta = 0.002$. We notice from this figure that the secrecy throughput of system with $\lambda_2 = 5\lambda_1$ is larger than that with $\lambda_2 = 3\lambda_1$. As there are more BSs available for CoMP transmission, secrecy throughput of the network increases.

To explain the effects of deploying PBSs with various channel estimation capacity, we compare the curves of $\rho_2 = 1, \lambda_2 = 5\lambda_1$ with $\rho_2 = 0.8, \lambda_2 = 8\lambda_1$ when the system works with the proposed transmission scheme, i.e., $\tau = 0.001, \theta = 0.002$. Note that PBSs with high channel estimation accuracy have higher secrecy throughput when the eavesdroppers' density is not quite large than BSs. However, when the eavesdroppers' density becomes quite large, PBSs with high density have higher secrecy throughput, even with worse channel estimation capacity. This implies that channel estimation is of paramount importance, and the channel estimation capability of PBSs should be taken into consideration when deploying them in macrocells. Therefore, it can help the designers of real dense HCNs to improve reliability and security performance by appropriate selecting PBSs density with consideration of the channel estimation capability of PBSs.

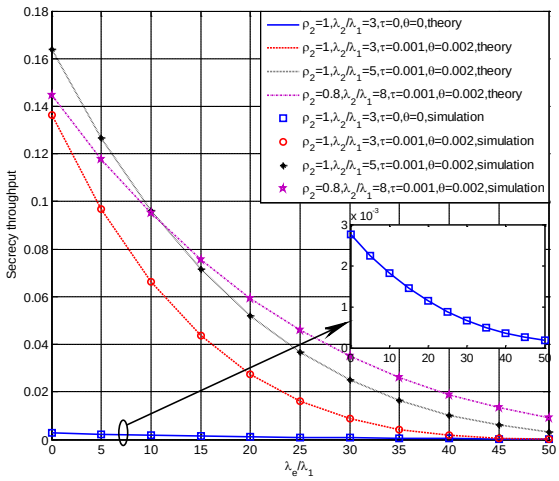

Fig. 9. Secrecy throughput versus eavesdroppers' density

6. Conclusion

In this paper, we investigate a CoMP transmission scheme based on dual-threshold optimization to improve the reliability and security performances of dense HCNs with imperfect CSI, which contains a candidate BSs formation policy and a CoMP networking strategy. In the candidate BSs formation policy, we introduce an access threshold τ and compare the received ARSPs with τ. Only BSs with good channel conditions can be opted as candidate BSs, which greatly increases access efficiency. In the CoMP networking strategy, we suggest a networking threshold θ and select serving BSs only when users received IESPs are larger than θ. Based on the proposed scheme, qualities of communication links are improved, thus reliable and secure communication is guaranteed. Then, we analyze the performance of the proposed scheme in terms of average achievable rate, COP and SOP. To

further support the performance of the network, we present a dual-threshold optimization model and a two-dimensional search method to obtain the optimal thresholds. Numerical results are presented to verify our theoretical analysis, and certify the proposed scheme can increase secrecy throughput by at most 0.13 bit/s/Hz, which draw a conclusion that the proposed CoMP transmission scheme can ensure reliable and secure communication in dense HCNs with imperfect CSI.

In addition, the calculation delay for selecting BSs for CoMP transmission needs to be considered in actual application and deployment. When the number of BSs is large, the algorithm has a large delay. The effectiveness of the algorithm is limited by different services. For example, the video media services need low delay but low security. Nevertheless, for data service, secure communication is more emphasis. Therefore, the current business requirements of real-time and security need to be considered when applying the proposed algorithm in actual deployment. Our future work may focus on designing an algorithm that considers both timeliness and security at the same time, to meet the needs of different communication services.

Appendix

A. Proof of Theorem 1

Proof: The difficulty of solving (14) is how to derive $R_u^{L|\{n_1,n_2,\cdots,n_K\}}$, hence we now first derive the expression of $R_u^{L|\{n_1,n_2,\cdots,n_K\}}$. The expression of $\mathbb{E}\left(1/SINR_u^{\{n_1,n_2,\cdots,n_K\}}\right)$ can be given by:

$$\mathbb{E}\left(1/SINR_u^{\{n_1,n_2,\cdots,n_K\}}\right)=\mathbb{E}\left(\frac{I_{io}+I_{IS}+I_{lo}+{\sigma_u}^2}{\left|\sum_{i=1}^{K}\sum_{t=1}^{n_i}\sqrt{P_i}\left\|X_{i,t}\right\|^{-\frac{\alpha}{2}}\tilde{h}_{i,t}\right|^2}\right)=\frac{\mathbb{E}\left(I_{io}+I_{IS}+I_{lo}+{\sigma_u}^2\right)}{\mathbb{E}\left(\left|\sum_{i=1}^{K}\sum_{t=1}^{n_i}\sqrt{P_i}\left\|X_{i,t}\right\|^{-\frac{\alpha}{2}}\tilde{h}_{i,t}\right|^2\right)} \tag{A1}$$

where

$$\mathbb{E}\left(I_{io}\right)=\sum_{i=1}^{K}\mathbb{E}\left(P_i\left|X_{i,t}\right|^{-\alpha_i}\left|o_{i,t}\right|^2\right)=\sum_{i=1}^{K}\int_0^{\infty}\frac{P_i}{1-\rho_i}\frac{2}{D_i^2}x^{-\alpha_i+1}dx=\sum_{i=1}^{K}\frac{2P_i}{D_i^2\left(1-\rho_i\right)\left(\alpha_i-2\right)} \tag{A2}$$

$$\mathbb{E}\left(I_{IS}\right)=\sum_{l=1}^{K}\mathbb{E}\left(P_l\left\|Z_{l,u}\right\|^{-\alpha_l}\left\|\tilde{h}_{l,u}\right\|^2\right)=\sum_{l=1}^{K}\sum\nolimits_{B_{l,u}\in\Upsilon^c}\int_0^{\infty}\left\{\left\|\tilde{h}_{l,u}\right\|^2>\left\|Z_{l,u}\right\|^{-\alpha_l}P_l^{-1}t\right\}dt=\sum_{l=1}^{K}\frac{2\pi\lambda_l P_l}{D_l^2\rho_l\left(\alpha_l-2\right)} \tag{A3}$$

$$\mathbb{E}\left(I_{lo}\right)=\sum_{l=1}^{K}\mathbb{E}\left(P_l\left\|Z_{l,u}\right\|^{-\alpha_l}\left\|o_{l,u}\right\|^2\right)=\sum_{l=1}^{K}\int_0^{\infty}\frac{P_l}{1-\rho_l}\frac{2}{D_l^2}x^{-\alpha_l+1}dx=\sum_{l=1}^{K}\frac{2P_l}{D_l^2\left(1-\rho_l\right)\left(\alpha_l-2\right)} \tag{A4}$$

$$\mathbb{E}\left(\left|\sum_{i=1}^{K}\sum_{t=1}^{n_i}\sqrt{P_i}\left\|X_{i,t}\right\|^{-\frac{\alpha}{2}}\tilde{h}_{i,t}\right|^2\right)=\sum_{i=1}^{K}\sum_{t=1}^{n_i}\mathbb{E}\left(P_i\left\|X_{i,t}\right\|^{-\alpha_i}\left\|\tilde{h}_{i,t}\right\|^2\right)=\sum_{i=1}^{K}\frac{2P_i n_i}{D_i^2\rho_i\left(\alpha_i-2\right)} \tag{A5}$$

Substituting $\mathbb{E}\left(1/SINR_u^{\{n_1,n_2,\cdots,n_K\}}\right)$ into (14), we can have the expression of $R_u^{L|\{n_1,n_2,\cdots,n_K\}}$:

$$R_u^{L|\{n_1,n_2,\cdots,n_K\}}=\log_2\left(1+\frac{\sum_{i=1}^{K}\frac{2P_i n_i}{D_i^2\rho_i\left(\alpha_i-2\right)}}{\sum_{i=1}^{K}\frac{2P_i}{D_i^2\left(1-\rho_i\right)\left(\alpha_i-2\right)}+\sum_{l=1}^{K}\frac{2P_l\left[\rho_l+\pi\lambda_l\left(1-\rho_l\right)\right]}{D_l^2\left(1-\rho_l\right)\rho_l\left(\alpha_l-2\right)}+{\sigma_u}^2}\right) \tag{A6}$$

Plugging (A6) into (15), we can obtain the lower bound of R_u in Theorem 1.

B. Proof of Theorem 2

Proof: The difficulty of solving (19) is how to derive $P_c^{\{n_1,n_2,\cdots,n_K\}}$. Therefore, we first derive the expression of $P_c^{\{n_1,n_2,\cdots,n_K\}}$. According to the definition of $P_c^{\{n_1,n_2,\cdots,n_K\}}$ in (18), we can have:

$$\begin{aligned}
&P_c^{\{n_1,n_2,\cdots,n_K\}} \\
&\overset{(a)}{=} \mathbb{E}_{X_{i,t}}\left\{\frac{1}{\rho_i}\exp\left(-\gamma\left(I_{io}+I_{lS}+I_{lo}+\sigma_u^2\right)[\chi]^{-1}\right)\right\} \\
&\overset{(b)}{=} \mathbb{E}_{X_{i,t}}\left\{\prod_{i=1}^{K}\frac{1}{\rho_i}\mathcal{L}_{I_{io}}\left(\gamma[\chi]^{-1}\right)\prod_{l=1}^{K}\mathcal{L}_{I_{ls}}\left(\gamma[\chi]^{-1}\right)\mathcal{L}_{I_{lo}}\left(\gamma[\chi]^{-1}\right)\exp\left(-\gamma\sigma_u^2[\chi]^{-1}\right)\right\} \\
&= \underbrace{\int\cdots\int}_{\boldsymbol{x}_1,\cdots,\boldsymbol{x}_K}\left\{\prod_{i=1}^{K}\frac{1}{\rho_i}\mathcal{L}_{I_{iN}}\left(\gamma[\chi]^{-1}\right)\prod_{l=1}^{K}\mathcal{L}_{I_{ls}}\left(\gamma[\chi]^{-1}\right)\mathcal{L}_{I_{lo}}\left(\gamma[\chi]^{-1}\right)f_{\boldsymbol{x}_i}\right\}\exp\left(-\gamma\sigma_u^2[\chi]^{-1}\right)d\boldsymbol{x}_1,\cdots,d\boldsymbol{x}_K
\end{aligned} \tag{B1}$$

where (a) follows from the fact that $\left|\sum_{i=1}^{K}\sum_{t=1}^{N_i}\sqrt{P_i}\left|X_{i,t}\right|^{-\frac{\alpha_i}{2}}\tilde{h}_{i,t}\right|^2$ is exponentially distributed with mean $\sum_{i=1}^{K}\sum_{t=1}^{N_i}\rho_i P_i\left|X_{i,t}\right|^{-\alpha_i}$ under the assumption that all the small-scale channel fading is the Rayleigh fading [27], and the fact that $\left(\tilde{h}_{i,1},\cdots,\tilde{h}_{i,N_i}\right)$ are mutually independent. (b) follows from the Laplace transform of I_{io}, I_{lS} and I_{lo}, i.e., $\mathcal{L}_{I_{io}}(s)=\exp(-sI_{io})$, $\mathcal{L}_{I_{lS}}(s)=\exp(-sI_{lS})$ and $\mathcal{L}_{I_{lo}}(s)=\exp(-sI_{lo})$.

Using the probability generating functional (PGFL), the Laplace transform $\mathcal{L}_{I_{io}}\left(\gamma[\chi]^{-1}\right)$ can be derived as:

$$\begin{aligned}
\mathcal{L}_{I_{io}}\left(\frac{\gamma}{\chi}\right) &= \mathbb{E}\left\{\exp\left\{-2\pi\lambda_i\int_0^{\infty}\left[y\Big/\left[1+\left(\frac{(1-\rho_i)\gamma P_i}{\chi}\right)^{-1}x^{\alpha_i}\right]\right]dx\right\}\right\} \\
&\overset{(a)}{=} \exp\left\{-\pi\lambda_i\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\left(\frac{(1-\rho_i)\gamma P_i}{\chi}\right)^{2/\alpha}\right\}
\end{aligned} \tag{B2}$$

where (a) is obtained under the assumption that $\alpha_i=\alpha_l=\alpha$. Similar to $\mathcal{L}_{I_{io}}\left(\frac{\gamma}{\chi}\right)$, $\mathcal{L}_{I_{lS}}\left(\frac{\gamma}{\chi}\right)$ and $\mathcal{L}_{I_{lo}}\left(\frac{\gamma}{\chi}\right)$ can be derived as:

$$\mathcal{L}_{I_{lS}}\left(\frac{\gamma}{\chi}\right) = \exp\left\{-\pi\lambda_l\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\left(\frac{\rho_l\gamma P_l}{\chi}\right)^{2/\alpha}\right\} \tag{B3}$$

$$\mathcal{L}_{I_{lo}}\left(\frac{\gamma}{\chi}\right) = \exp\left\{-\pi\lambda_l\Gamma\left(1+\frac{2}{\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)\left(\frac{(1-\rho_l)\gamma P_l}{\chi}\right)^{2/\alpha}\right\} \tag{B4}$$

Combing (B1) and (19) together, we can obtain the expression of P_{co} in Theorem 2.

References

[1] Wang CX, Haider F, Gao X, et al, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 122-130, 2014. Article (CrossRef Link).

[2] Yang X and Fapojuwo AO, "Coverage probability analysis of heterogeneous cellular networks in rician/rayleigh fading environments," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1197-1200, 2015. Article (CrossRef Link).

[3] Wang HM, Zheng TX, Yuan J, et al, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204-1219, 2016. Article (CrossRef Link).

[4] Wu H, Tao X, Li N, et al, "Secrecy outage probability in multi-rat heterogeneous networks," *IEEE Communications Letters*, vol. 20, no. 1, pp. 53-56, 2016. Article (CrossRef Link)

[5] Zheng TX, Wang HM, Lee MH, "Multi-antenna transmission in downlink heterogeneous cellular networks under a threshold-based mobile association policy," *IEEE Transactions on Communications*, vol. 65, no. 1, pp. 244-256, 2017. Article (CrossRef Link).

[6] Lv T, Gao H, Yang S, "Secrecy transmit beamforming for heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1154-1170, 2015. Article (CrossRef Link).

[7] Yan S, Shang Y, Zhang X, et al, "An artificial noise scheme for secure communication in heterogeneous D2D and cellular networks," in *Proc. of Vehicular Technology Conference (VTC-Fall)*, 2017 IEEE. Article (CrossRef Link).

[8] Zhong Z, Luo W, Peng J, et al, "Secrecy performance analysis of cooperative transmission and co-operative jamming for multi-tier heterogeneous cellular networks," *Science China Information sciences*, vol. 46, no. 1, pp. 33-48, 2016. Article (CrossRef Link).

[9] Zheng TX, Yang Q, Zhang Y, et al, "Physical layer security in distributed wireless networks using full-duplex receiver jamming," in *Proc. of Globecom Workshops*, 2017 IEEE. Article (CrossRef Link).

[10] Saeed Sheikhzadeh, Mohammad R. Javan and Nader Mokari, "Radio resource allocation for physical-layer security in OFDMA based HetNets with unknown mode of adversary," in *Proc. of Communication and Information Theory (IWCIT)*, 2017 IEEE, pp. 1-5, 2017. Article (CrossRef Link).

[11] Huang J, Yin Y, Zhao Y, et al. "A Game-Theoretic Resource Allocation Approach for Intercell Device-to-Device Communications in Cellular Networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 4, pp. 475-486, 2016. Article (CrossRef Link).

[12] Huang J, Hang S, Xing C, et al, "Game-Theoretic Power Control Mechanisms for Device-to-Device Communications Underlaying Cellular System," *IEEE Transactions on Vehicular Technology*, 2018, in print. Article (CrossRef Link).

[13] Huang J, Xing C C, Qian Y, et al. "Resource Allocation for Multi-cell Device-to-Device Communications Underlaying 5G Networks: A Game-Theoretic Mechanism with Incomplete Information," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2557-2570, 2018. Article (CrossRef Link).

[14] Wang HM, Wang C, Zheng TX, et al, "Impact of artificial noise on cellular networks: a stochastic geometry approach," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7390-7404, 2016. Article (CrossRef Link).

[15] Zheng TX and Wang HM, "Optimal power allocation for artificial noise under imperfect csi against spatially random eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8812-8817, 2016. Article (CrossRef Link).

[16] Mu P, Li Z and Wang B, "Secure on-off transmission in slow fading wiretap channel with imperfect CSI," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9582-9586, 2017. Article (CrossRef Link).

[17] He B, Zhou X, "Secure on-off transmission design with channel estimation errors," *IEEE Transactions on Information Forensics Security*, vol. 8, no. 12, pp. 1923-1936, 2013. Article (CrossRef Link).
[18] Mukherjee A and Swindlehurst A L, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351-361, 2010. Article (CrossRef Link).
[19] Al-Hraishawi H, Baduge G and Schaefer R, "Artificial noise-aided physical layer security in underlay cognitive massive MIMO systems with pilot contamination," *Entropy*, vol. 19, no. 7, pp. 349-370, 2017. Article (CrossRef Link).
[20] Tourki K, Hasna M O, "Proactive spectrum sharing incentive for physical layer security enhancement using outdated CSI," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6273-6283, 2016. Article (CrossRef Link).
[21] Chen X, Chen HH, "Physical layer security in multi-cell miso downlinks with incomplete CSI-a unified secrecy performance analysis," *IEEE Transactions on Signal Processing*, vol. 62, no. 23, pp. 6286-6297, 2014. Article (CrossRef Link).
[22] Wang W, Lv T and Gao H, "Robust beamforming and power allocation for secrecy in DF relay networks with imperfect channel state information," *IEEE Access*, vol. 1, no. 1, pp. 9520-9527, 2017. Article (CrossRef Link).
[23] Li B, Fei Z, and Chen H, "Robust artificial noise-aided secure beamforming in wireless-powered non-regenerative relay networks," *IEEE Access*, vol. 4, pp. 7921-7929, 2016. Article (CrossRef Link).
[24] Li B and Fei Z, "Robust beamforming and cooperative jamming for secure transmission in DF relay systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 68, no. 1, pp. 1-11, 2016. Article (CrossRef Link).
[25] Wang L, Cai YM, Zou YL, et al, "Joint relay and jammer selection improves the physical layer security in the face of csi feedback delays," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6259-6274, 2016. Article (CrossRef Link).
[26] D. Lee, H. Seo, B. Clerckx, et al, "Coordinated multipoint transmission and reception in LTE-Advanced: deployment scenarios and operational challenges," *IEEE Communications Magazine*, vol. 50, no. 2, pp. 148-155, 2012. Article (CrossRef Link).
[27] Nigam G, Minero P and Haenggi M, "Coordinated multipoint joint transmission in heterogeneous networks," *IEEE Transactions on Communications*, vol. 62, no. 11, pp. 4134-4146, 2014. Article (CrossRef Link).
[28] Wang Y, Liang B and Xu Y, "A two-stage rank selection scheme in downlink CoMP transmission networks," in *Proc. of IEEE International Conference on Communications (ICC)*, 2016 IEEE, pp.1-6, 2016. Article (CrossRef Link).
[29] Xu M, Tao X, Yang F, et al, "Enhancing secured coverage with comp transmission in heterogeneous cellular networks," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2272-2275, 2016. Article (CrossRef Link).
[30] B. Hassibi and B. Hochwald, "How much training is needed in multipleantenna wireless links?" *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp.951-963, 2003. Article (CrossRef Link).
[31] Jo HS, Sang YJ, Xia P, et al, "Heterogeneous cellular networks with flexible cell association: a comprehensive downlink SINR analysis," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3484-3495, 2011.Article (CrossRef Link).

XU Yunjia, is currently a M.S. candidate at National Digital Switching System Engineering & Technological Research Center, Henan, China. She received the B.E. Degree in information and communication engineering from information and engineering University, Zhengzhou, China, in 2015. Her major research interests include physical layer security, dense heterogeneous cellular networks and imperfect channel state information.

HUANG Kaizhi, received her Ph.D. degree in communication and information system from Tsinghua University, Beijing, China. Now, she is a professor and supervisor of postgraduate student in National Digital Switching System Engineering & Technological Research Center, Henan, China. She is also serving as a leader of Wireless Mobile Communication Innovation Technology Team of Henan. Her major research interests include wireless mobile communication network and information secrecy.

HU Xin, is currently a M.S. candidate at National Digital Switching System Engineering & Technological Research Center, Henan, China. He received the B.E. Degree in technique and instrumentation of measurements from Xi'an Jiaotong University, Xi'an, China, in 2015. His major research interests include physical layer security in simultaneous wireless information and power transfer.

ZHOU Yi, is currently a M.S. candidate at National Digital Switching System Engineering & Technological Research Center, Henan, China. He received the B.E. Degree in information and communication engineering from information and engineering University, Zhengzhou, China, in 2014. His major research interests include physical layer security and relay communication.

CHEN Yajun, received the B.E. and M.S. degrees in University of Electronic Science and Technology of China and National Digital Switching System Engineering & Technological R&D Center (NDSC), respectively. He is currently a Ph.D. candidate at NDSC, Zhengzhou, China. His research interests include physical layer security, wireless location and resource management in 5G networks.

JIANG Wenyu, is currently a M.S. candidate at National Digital Switching System Engineering & Technological Research Center, Henan, China. He received the B.E. Degree in information and communication engineering from Shanghai Jiaotong University, Shanghai, China, in 2017. His major research interests include physical layer security with imperfect channel state information.