SCIENCE CHINA
Information Sciences

December 2020, Vol. 63 220304:1–220304:14
https://doi.org/10.1007/s11432-019-2836-0

• RESEARCH PAPER •
Special Focus on Challenges and New Insights for Network Security in 5G-and-Beyond

Secure transmission for heterogeneous cellular network with limited feedback

Wenyu JIANG, Kaizhi HUANG*, Shuaifang XIAO & Xiaoming XU

PLA Strategic Support Force Information Engineering University, Zhengzhou 450002*, China*

Received 30 November 2019/Accepted 16 March 2020/Published online 11 November 2020

Abstract We study physical layer secure transmission with limited feedback in heterogeneous cellular networks. A transmission protocol is designed to obtain more secure and accurate channel state information (CSI) for enhancing the secrecy performance. Under the proposed protocol, we derive expressions of coverage probability and secrecy outage probability to analyze the security performance with different system parameters such as feedback CSI length and number of antennas. Furthermore, an iteration algorithm is proposed to balance the tradeoff between the feedback and transmission time, and maximize the average secrecy throughput under coverage and secrecy outage constrains. Numeric results demonstrate the optimal feedback overhead and the maximum average secrecy throughput are influenced by the number of antennas.

Keywords physical layer security, heterogeneous cellular networks, limited feedback, secure transmission, average secrecy throughput

Citation Jiang W Y, Huang K Z, Xiao S F, et al. Secure transmission for heterogeneous cellular network with limited feedback. Sci China Inf Sci, 2020, 63(12): 220304, https://doi.org/10.1007/s11432-019-2836-0

1 Introduction

Heterogeneous cellular networks (HCNs) have become a promising approach in 5G network which demands high data rate and wide coverage. The infrastructure in HCNs is classified into different types such as macro, micro, and home base stations (BS) according to the deployment locations and equipment parameters [1]. Generally, the macro BSs provide wide coverage and large scale access. The low power nodes (LPNs) such as micro BSs located in hot spot or uncovered area result in more comprehensive coverage area and higher spectral efficiency.

Generally, BSs always use the open access mechanism in order to sever more users, which is widely accepted by the most of network operators in the world. In other words, users are allowed to access each BS without restriction. However, due to the open architecture and broadcast nature of HCNs, the private information sending by BSs is more vulnerable to be eavesdropped. The eavesdroppers (Eves) close to the BS are easier to decode the secrecy information than the users in overlapping coverage areas of different type BSs. Ghosh et al. [1] pointed out that it is necessary to involve the security in HCNs, and the security problem in HCNs has been gradually recognized.

Physical layer security (PLS) technology, utilizing endogenous security of wireless channels to transmit private information, can effectively improve the security performance in the wireless communication. Beginning with Wyner's research on wire-tapping model [2], recent years researches on PLS have gradually expanded to multi-users [3,4] and multi-cells networks [5,6], and an amount of PLS schemes and methods have been proposed.

* Corresponding author (email: huangkaizhi@tsinghua.org.cn)

1.1 Related work

Early PLS researches focused on the ideal three-point model. With the advent of stochastic geometry theory, Ref. [7] uses it as a powerful tool for studying the average performance of the wireless communication system. Under the stochastic geometric model in multi-antenna system, secure transmission schemes are designed where Eves distributed as a poisson point process (PPP) in [8–10]. The average secrecy outage probability was proposed to investigate the system security performance in multiple-input single-output (MISO) and multiple-input multiple-output (MIMO) scenario respectively. Furthermore, ElSawy et al. [11] extended the stochastic geometric framework into the cellular network where BSs and the users both obey the PPP distribution. Wang et al. [12] evaluated the security performance under several assumptions on the Eve's location in MISO system. The location distribution and signaling overhead were analyzed to improve the available secrecy rate. However, they did not consider the small-scale fading, and ignore the inter-layer interference. Motivated by [12], the contribution [13] proposed a tractable approach to analyze the physical-layer security in the down-link of a multi-tier HCN, and focused on the upper and lower bound of secrecy coverage probability with inter and intra layer interference. Further research on network construction, the optimal BS density was derived for maximizing the secrecy rate in [14], where other users were seen as potential Eves.

The PLS transmission schemes mentioned above require complete channel state information (CSI) at BS, especially channel direction information (CDI) to design a precoding matrix. The system which cannot directly extract CSI by channel reciprocity, like frequency division duplex (FDD) system, always gets CSI from the feedback by the user equipment (UE) to form a close-loop transmission. Owing to the limitation of feedback channel's capacity, UE needs to compress the estimation CSI into a few quantized information before feedback. So this method is called limited-rate feedback or limited feedback technique [15], and has been widely used in multi-antenna communication systems. At present, the codebook-based limited feedback technique is generally employed to reduce the feedback length of CSI in cellular networks. The element in codebook which has highest correlation with the estimated CSI can effectively represents the down-link CSI. Obviously, a large scale codebook is benefit for the accuracy of feedback CSI but makes the throughput gain small. Zhang et al. [16, 17] investigated the minimum feedback length under the constraint of secrecy outage probability, and the power allocation coefficient of the artificial noise and beamforming signal to obtain the maximum secrecy throughput. The author in [18] proposed an algorithm to determine the tradeoff between training and feedback overhead, and measured the maximum average secrecy throughput.

At present, most PLS schemes in HCNs are not specific designed for the FDD systems which cannot directly use the reciprocity to obtain CSI. The traditional limited feedback technique is not favorable for the HCNs. Firstly, BSs in the HCN overlap each other in the HCNs, which makes the beamforming or artificial noise cause more interference with CSI error, and the feedback capacity be susceptible by other uplink signals. Secondly, the heterogeneous BSs make the design of the feedback length different from the traditional single-layer network. Different transmit power and the number of antennas will influence feedback overhead [19]. Besides, most limited feedback researches avoid the issue of feedback security which is easily happened because of the weakness of the UE. These new issues call for specific secure transmission scheme and analysis in HCNs with limited feedback.

1.2 Our contribution

This study first proposes a PLS transmission protocol in K-tier HCN with limited feedback. By explicitly considering the feedback overhead in different tier, the expressions of coverage probability and secrecy outage probability under imperfect CSI are derived. The influence of the number of antennas, density of the BS and other system parameters on the security performance are analyzed. Finally we design an iteration algorithm to examine the optimal fraction of resource allocated to feedback overhead and data transmission. The contributions are summarized as follows:

(1) We establish a PLS transmission protocol for K-tier HCNs with limited feedback. The whole coherent time is divided into the training period, secret key generate period, CSI feedback period and data

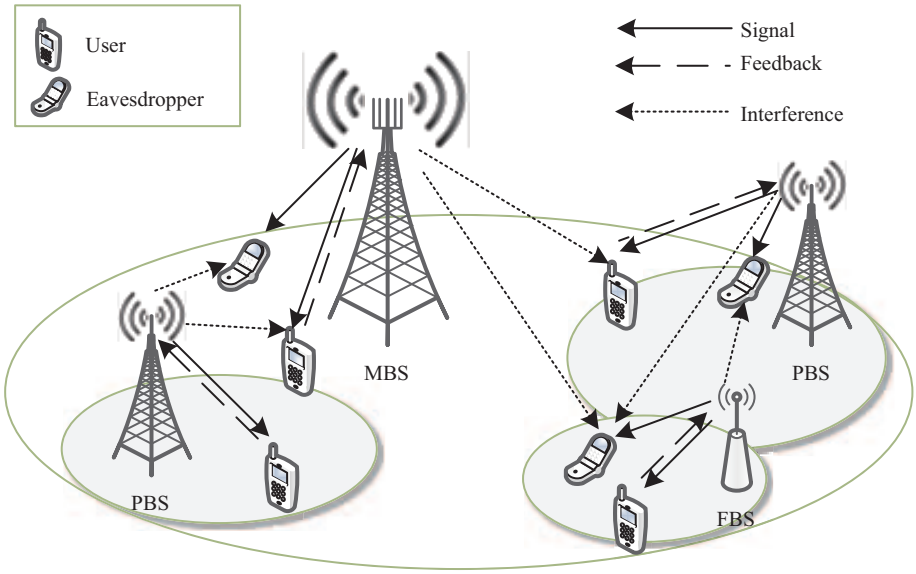

Figure 1 (Color online) An illustration of 3-tier HCN down-link transmission with feedback coexist with eavesdroppers.

transmission period. The four-periods transmission protocol helps the transmitter obtain the receiver's CSI to perform precoding matrix. PLS key generation is introduced into the protocol to protect the feedback security. And a variable feedback length scheme is designed to improve the efficiency of feedback period.

(2) We propose a new integral representation for the coverage probability and secrecy outage probability when there are both estimation and feedback errors. Firstly we obtain the expression of coverage probability which is defined as the probability that the capacity of the channel meets the demand rate. We find that the variable feedback CSI length can increase the coverage probability. The secrecy outage probability which is defined as the probability that an arbitrary Eve's capacity is larger than the redundant rate is also analyzed. Then the asymptotic analyze reveals the influence of the antenna number and feedback length on these security performance.

(3) We design an iteration algorithm to optimize user average secrecy throughput (AST) under the coverage and secrecy outage constraints. The optimal problem is divided into two subproblems. First considering the tradeoff between feedback and data transmission during a time slot, we search the optimal feedback length by changing the amount of feedback in each tier. Next, for maximizing the network's secrecy throughput, the coding parameters are adjusted by the algorithm. The result shows that a large antenna number is not always beneficial to the average secrecy throughput.

The remainder of this paper is organized as follows. In Section 2, we describe the system model. The coverage probability and secrecy outage probability under the specific transmission protocol are given in Section 3. In Section 4, we evaluate the average secrecy throughput. The numeric results are shown in Section 5. Finally, we conclude our work in Section 6.

2 System model

We consider a K-tier FDD HCN existing Macro base stations (MBSs), Pico base stations (PBSs), Femto base stations (FBSs), which have different operating parameters, as illustrated in Figure 1. The BSs in tier-i, expressed as B_i, are distributed according to homogeneous PPP with density λ_i in the 2-dimensional space R^2. The coexisting single antenna users and Eves subject to PPP distribution with densities λ_u and λ_e, respectively. For convenience, the set of BSs in tier-i, users and Eves are defined as θ_i, θ_u, and θ_e, respectively. The target user represented by U_x receives the confidential message, while the malicious Eve attempt to intercept the secure information without collaboration.

2.1 Distribution model

The open-access scenario which means that users are allowed to access arbitrary BS in each tier. While, the users obey the baseline designed in the FDD cellular network. In the cell search process, according to the primary synchronization signal (PSS) strength at the fixed frequency, the user can determine the optimal BS to access, represented by B_{io}. According to [20], the probability of the user accessing the tier-i BS is

$$\mathcal{A}_i = 2\pi\lambda_i \int_0^{\infty} x \exp\left\{-\pi \sum_{j=1}^{K} \lambda_j \left(\frac{P_j}{P_i}\right)^{2/\alpha_j} x^{2\alpha_i/\alpha_j}\right\} \mathrm{d}x. \tag{1}$$

The distance between the accessed BS with user is

$$f_{X_i}(x) = \frac{2\pi\lambda_i}{\mathcal{A}_i} x \exp\left\{-\pi \sum_{j=1}^{K} \lambda_j \left(\frac{P_j}{P_i}\right)^{2/a_j} x^{2a_i/a_j}\right\}. \tag{2}$$

Obviously, the first problem that needs to be solved in HCNs is interference. The current inter-cell interference coordination (ICIC) scheme mainly uses frequency reuse technology such as partial frequency reuse (FFR) and soft frequency reuse (SFR). Since the FDD cellular system do not suffer from the neighbor BS's interference a lot. However, in the heterogeneous network, the stochasticity of the BS's location leads that the distance between co-frequencies BS becomes closer. In order to characterize the randomness of interference, we assume that λ_i is the density after frequency reuse designing. What's more, the BS will stand by without users, the activation probability is defined as $\mathcal{V}_i = 1 - \exp(-2\pi\lambda_u \mathcal{A}_i)$ in [18]. The set of active BSs in tier-i is a subset of θ_i, defined as θ_i^a with density $\lambda_i^a = \lambda_i \mathcal{V}_i$, which will have an impact on the interference of the system.

2.2 Channel estimation and feedback

Wireless channel in HCN is modeled as the quasi-static Rayleigh block fading together with the large scale path loss governed by exponent α. The channel from optimal BS B_{io} with the target user U_x is characterized by $h_{io} x_{io}^{-\alpha}$. The $h_{io} \in C^{N_i \times 1}$ denotes the coefficient vector caused by the small scale fading, and the x_{io} denotes the spatial distance. The illustration of channel estimation and feedback is shown in Figure 2.

2.2.1 *Channel estimation*

When UE receives the pilot sequences from all transmitter's antenna, the user estimates the channel using a minimum mean square error (MMSE) method, expressed as h_i. Owing to the interference from other similar pilot sequences, the estimated error can be expressed as

$$h_i = \sqrt{1 - \sigma_m^2}\hat{h}_i + \sigma_m^2 m_i, \tag{3}$$

while the σ_m represents the estimation error parameter which is related to the transmit antenna numbers and the signal to interference plus noise ratio (SINR) at the receiver [19]. The estimation result $\hat{h}_i$ and estimation error m_i contain i.i.d. complex Gaussian variable elements, satisfying $\hat{h}_i \sim \mathcal{CN}(0, I_{N_i})$ and $m_i \sim \mathcal{CN}(0, I_{N_i})$, respectively. We assume that the σ_m is fixed in all layer and maintain stability during the whole communication. Since the training signal is transmitted as broadcast, the Eves are able to obtain the accurate CSI.

2.2.2 *limited feedback of CDI*

After the user obtains the channel estimation vector $\hat{h}_i$, the user will compress the matrix into a few bits using the private codebook. The codebook-based limited feedback technique generally uses the random vector quantization (RVQ) method to generate the codebook [21]. We follow this criterion to analyze the quantization error caused by the compress.

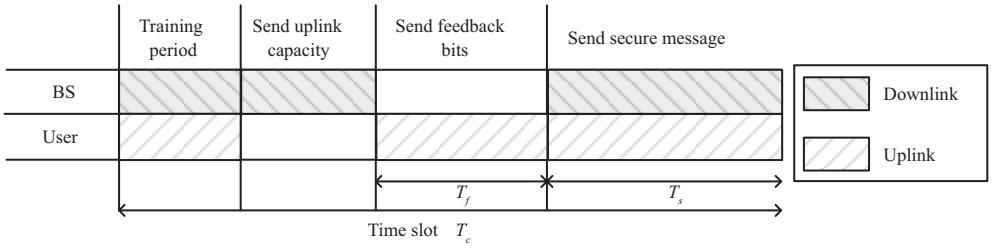

Figure 2 (Color online) Scheduling period partition of a specific time slot in proposed transmission protocol.

The feedback information for tier-i BS contains B_i bits, and is associated with the specific CDI vector index in the codebook $\mathcal{C}$ of size 2^{B_i}. Each element in the codebook is an i.i.d. isotropic unit-form vector on the complex hypersphere [22]. The optimal element in the codebook $h_{\hat{l}}$ is selected as follows:

$$h_{\hat{l}} = \arg\max_{h_l \in \mathcal{C}} |h_l^H \tilde{h}_i|^2, \tag{4}$$

where $\tilde{h}_i = \hat{h}_i / ||\hat{h}_i||^2$ represents normalized channel vector or CDI. With the criterion mentioned above, we define $|h_l^H \tilde{h}|^2$ as the quantity of the feedback CSI. The cumulative distribution function (CDF) of $|h_l^H \tilde{h}|^2$ is given by [17]

$$F(x) = \begin{cases} 0, & 0 \leqslant x < 1-\varepsilon, \\ 1 - 2^{B_i}(1-x)^{N_i-1}, & 1-\varepsilon \leqslant x \leqslant 1, \end{cases} \tag{5}$$

where $\varepsilon = 2^{-\frac{B_i}{N_i-1}}$ represents the maximum quantization error of the user. Considering the issue of eavesdropping during feedback, we find that the uplink transmission will be easily tapped due to the weak capability of the UE. The limit of transmit antenna and power restricts the performance of beamforming and artificial-noise scheme. Therefore, the PLS encryption method, which extracts a key from the source such as angel of arrival (AOA) or multipath delay in a non-reciprocal channel, can effectively encrypt the uplink feedback channel. The authors in [23, 24] have studied on PLS encryption in an FDD system, and implied that the key generation rate could not be high. It is still acceptable for this low rate requirement scenario because the feedback length is very small.

3 Transmission protocol and performance analysis

In this section, a secure transmission protocol for FDD HCNs is proposed in order to protect the down-link security. Existing limited feedback technology uses fixed feedback length, which is not adapt to various BS configurations and feedback requirements for HCNs. The other fatal problem is that the feedback may also be eavesdropped by the unauthorized users, which makes the CSI disclosed and invalidates the transmission scheme. Therefore, we have designed a transmission protocol with variable and secret feedback. The transmission protocol is described as follows:

(1) The BS and the user send a training sequence for channel estimation. The existing long term evolution (LTE) protocol has indicated the training procedure in every sub-frame. The transmitter sequentially sends the training symbols for each antenna in the specific resource element. The user and BS respectively calculate the downlink and uplink CSI through channel estimation.

(2) The BS and users generate a secret key using the shared source such as AOA or multi-path delay from the calculated CSI. We utilize the secret key to encrypt the uplink channel with secure feedback information. It is important to point that key generate rate is not very high, which have more consistency to ensure the limited feedback's accuracy. According to the one-time-pad encryption, we assume that the key generate rate is R_{up}, that is, the max secure feedback rate is also R_{up}.

(3) The user compresses the CSI and sends the feedback information back. After receiving the pilot sequence from BS, the user estimates the down-link channel $\hat{h}_i$. According to the configuration of the current accessed BS and the obtained uplink channel capacity, an appropriate feedback length is chosen.

The index $\hat{l}$ of channel matrix with the highest similarity is selected from the codebook $\mathcal{C}$, and secure transmitted back to the BS with the help of secret key.

(4) During the remaining time, the user and BS transmits the uplink and down-link data. The BSs utilizes the maximum ratio combining (MRC) precoding matrix $w_i = h_{\hat{l}}$, where $h_{\hat{l}}$ is the feedback CDI at transmitter, to sever the legitimate user. What's more, we consider the worst scenario that the other active BS always contains users for efficiency reason, that is, the user and Eve will be interfered by all active BSs except the sever BS. The user's receive signal is

$$y_{u_x}=\sqrt{P_i(1-\sigma_m^2)}\hat{h}_{io}^H w_{io}|X_{io}|^{-\alpha}+\sqrt{P_i\sigma_m^2}m_{io}^H w_{io}|X_{io}|^{-\alpha}+\sum_{j=1}^{K}\sum_{jo\in\Theta_j^a,jo\neq io}(\sqrt{P_j}h_{jo}^H w_{jo}|Z_{jo}|^{-\alpha})+n_{io}, \quad (6)$$

where the X_{io} and Z_{jo} represent the distance of the setting BS and other BSs to the target user. n_{io} is the noise signal in the channel. In addition, existing articles mostly use artificial noise to improve the security performance. However the complex interference in the HCN is not in favor of sending noise. It is difficult for users and Eves to eliminate the interference. Therefore, maximizing the user channel quality advantage by using beamforming have more priority. We assume that the target user U_x is served by the BS $B_{i,o}$ in tier-i. Under the protocol above, we first analyze the coverage and secrecy outage performance of the HCNs with limited feedback.

3.1 Coverage probability

According to the received signal in (6), the instantaneous SINR of the U_x is written as

$$\mathrm{SINR}_u^i = \frac{P_i(1-\sigma_m^2)||\hat{h}_{io}||^2|\tilde{h}_{io}^H h_{\hat{l}}|^2|X_{io}|^{-\alpha_i}}{I_{\mathrm{err}}+I_{ui}+\sigma_u^2} \quad (7)$$

with $I_{\mathrm{err}} = P_i\sigma_m^2|m^H h_{\hat{l}}|^2|X_{io}|^{-\alpha_i}$ and $I_{ui} = \sum_{j=1}^{K}\sum_{jo\in\theta_j^a,jo\neq io}P_j\|h_{jo}\|^2|Z_{jo}|^{-\alpha_j}$, represent the interference caused by the CSI estimation error and the interference from the other BS. Where $|\tilde{h}_{io}^H h_{\hat{l}}|^2$ represents the feedback CDI quantity of the channel. We aim to use the statistical distribution of the numerator by applying the transform mentioned in [18] to derive the close-form expression of the coverage probability.

The user's average coverage probabilities of HCNs is considered to be the weighted average of the coverage probability of each layer:

$$p_c = \sum_{i=1}^{K}\mathcal{A}_i p_c^i. \quad (8)$$

And the coverage probability when the user access tier-i p_c^i are defined as the probability that the capacity of channel is larger than the code word rate R_b:

$$p_c^i = E_{r,I_{ui},I_{\mathrm{err}}}(P(\log_2(1+\mathrm{SNR}_u^i) > R_b)). \quad (9)$$

The difficulty in calculating the p_c^i is finding the distribution of SNR_u^i. However, it is nearly impossible to express the CDF of SNR_u^i, because of the independence of the interference coming from the inter-layer, intra-layer and the noise. So p_c^i is first transformed as

$$\begin{aligned} p_c^i &= E_{r,I_{\mathrm{err}},I_{ui}}(P(\mathrm{SNR}_u^i > 2^{R_b}-1)) \\ &= E_{r,I_{\mathrm{err}},I_{ui}}\left(P\left(||\hat{h}_{io}||^2|\tilde{h}_{io}^H h_{\hat{l}}|^2 > \frac{(2^{R_b}-1)(I_{\mathrm{err}}+I_{ui}+\sigma_u^2)}{P_i(1-\sigma_m^2)|X_{io}|^{-\alpha_i}}\right)\right). \end{aligned} \quad (10)$$

Define $||h_{io}^*||^2 = ||\hat{h}_{io}||^2|\tilde{h}_{io}^H h_{\hat{l}}|^2$ as the equivalent channel after beamforming with the imperfect CSI. In addition, $||\hat{h}_{io}||^2$ represents the channel gain information (CGI), which is independent with CDI. Therefore, we can derive the CDF of the $||h_{io}^*||^2$ as Lemma 1.

Lemma 1. The CDF of $||h_{io}^*||^2$ is derived as

$$P(||h_{io}^*||^2 \leqslant x) = \sum_{m=0}^{N_i-1}\frac{(\frac{x}{1-\varepsilon})^m \mathrm{e}^{-\frac{x}{1-\varepsilon}}(2^{B_i}\varepsilon^m-1)}{\Gamma(m+1)} + 1 - 2^{B_i}\mathrm{e}^{-x}. \quad (11)$$

Proof. the proof is given in Appendix A.

According to Lemma 1 and (10), we can derive the expression of p_c^i as

$$\begin{aligned} p_c^i &= E_{r,\lambda}(P(||h_{io}^*||^2 > \lambda)) \\ &= E_{r,\lambda}\left(2^{B_i}\mathrm{e}^{-\lambda} - \sum_{m=0}^{N_i-1} \frac{(\frac{\lambda}{1-\varepsilon})^m \mathrm{e}^{-\frac{\lambda}{1-\varepsilon}}(2^{B_i}\varepsilon^m - 1)}{\Gamma(m+1)}\right), \end{aligned} \tag{12}$$

where $K = \frac{(2^{R_b}-1)}{P_i|X_{iu}|^{-\alpha_i}(1-\sigma_m^2)}$, and $\lambda = K(I_{\mathrm{err}} + I_{ui} + \sigma_u^2)$. However, λ is still a random variable with complex distribution. In [20], the Laplace-transform is used to simplify the population mean. Similarly, we derive the approximation of coverage probability in Lemma 2.

Lemma 2. the coverage probability in tier-i is given by

$$p_c^i = \int_0^\infty \left(2^{B_i}\mathrm{e}^{-K\sigma_1^2}\mathcal{L}_{I_{ui}}(K) - \sum_{m=0}^{N-1}\sum_{p=0}^{m}\binom{m}{p}\Psi(m,p)\right) f_{X_i}(x)\mathrm{d}x, \tag{13}$$

where $\Psi(m,p)$ is

$$\Psi(m,p) = \frac{(-1)^m \mathcal{L}_{I_{ui}}^{(m)}(\frac{K}{1-\varepsilon})(\frac{K\sigma_1^2}{1-\varepsilon})^{m-p}\mathrm{e}^{-\frac{K\sigma_1^2}{1-\varepsilon}}(2^{B_i}\varepsilon^m - 1)}{\Gamma(m+1)}. \tag{14}$$

And $\mathcal{L}_{I_{ui}}^{(p)}(s)$ is the p-order Laplace transform of I_{ui}. Using [25], the expression of origin and p-order Laplace transform is given by

$$\mathcal{L}_{I_{ui}}(s) = \prod_{j=1}^{K}\exp\left(-\pi\lambda_j^o\sum_{k=1}^{N_j} sP_j\frac{x^{\alpha_j(2/\alpha_j-1)}}{(1-2/\alpha_j)}{}_2F_1\left(k, 1-2/\alpha_j; 2-2/\alpha_j; -\frac{1}{sP_jx^{-\alpha_j}}\right)\right), \tag{15}$$

$$\begin{aligned} \mathcal{L}_{I_{ui}}^{(p)}(s) = \sum_{z=0}^{p}\sum_{j=1}^{K}\pi\lambda_j^o\mathcal{L}_{I_{ui}}^{(z)}(s)\frac{(p-z)!(P_jx^{-\alpha_j})^{-N_j-1/\alpha_j}}{(P_j)^{-1/\alpha_j}s^{N_j+p-z}(N_j+1/\alpha_j)}{}_2F_1\Big(N_j+p-z, \\ N_j+1/\alpha_j; N_j+1/\alpha_j+1; -\frac{1}{sP_jx^{-\alpha_j}}\Big). \end{aligned} \tag{16}$$

Proof. The proof is given in Appendix B.

Although the above formula is very complicated, the hypergeometric function can easily obtain the numerical solution. Similarly, the p-order Laplace transform can be obtained by iteration. What's more, it is important for network design to figure out the influence of system parameters on the coverage probability, and the asymptotic analysis is provided to help us understand how p_c^i is affected by the system parameters.

Property 1. The coverage probability in tier-i decreases with the code-word rate R_b and P_j, and increases with the B_i and P_i. However, it is not influenced by other tiers' B_j.

Property 1 explains the effect of some system parameters on coverage probability. We can find that p_c^i is a complementary cumulative distribution function (CCDF) which is decreasing with independent variable. When N_i is fixed, $K\lambda$ will determine the trend. It is easy to find the property in the corresponding relationship by solving the partial derivative. We analyze the reason that the P_i determine the signal strength which is directly helpful for connection, and the increasing access probability make the interference from other tiers smaller. On the contrary, P_j from other tier will weaken the coverage probability in the same reason. In the system, when the feedback error is reduced, the beamforming is more accurate, so that the user can get the maximum gain without being exposed to the leakage.

Property 2. When P_1 is large and $\lambda_u \gg \lambda_j$, $j \neq 1$, the p_c^i is increasing with λ_1 and decreasing with λ_j.

When $\lambda_u \gg \lambda_j$, that is mainly all BSs are active, the interference will approach the upper bound. We can find that the I_{ui} in (7) will decrease as λ_j. When other variables stay fixed, p_c^i will reduce as interference grows up. We can also conjecture that when λ_u is small, the p_c will increase as λ_j because the remain BSs are active by users, which is analyzed in [20]. Under this property, some interesting insight into coverage probability is that the density of LPNs must depend on the amount of users.

Property 3. When $B_i \gg N_i$, the coverage probability is mainly influenced by the estimation error, and converges into a constant value.

When $B_i \gg N_i$, $\epsilon \to 0$, and the $p_c^i = 1 - F_\gamma(N_i, K\lambda)$, which is independent with B_i. With this assumption, the problem degenerates into the problem without limited feedback, which is analyzed in [26]. Obviously, the p_c^i will increase as the estimation accuracy increase. The property is further analyzed with the numeric result in Section 5.

3.2 Secrecy outage probability

Although the estimation error and the feedback error will influence the beamforming accuracy, the Eves will not detect the impact of the error in the probability perspective. The SINR is derived as

$$\mathrm{SINR}_e^i = \frac{P_i |\hat{h}_{ie}^H h_{\hat{l}}|^2 |Y_{ie}|^{-\alpha_i}}{I_{ei} + \sigma_e^2}. \tag{17}$$

For the passive Eve, it is difficult to calculate its instantaneous SINR at BS. Therefore, the secrecy outage probability (SOP) is generally used to describe the security degree of a system from the viewpoint of probability. Secrecy outage probability is given by the probability when the redundancy R_e is lower than the capacity of Eve's channel. In the HCN, Eves are randomly distributed in the system. The secrecy outage happens when the strongest Eve achieves the threshold:

$$\begin{aligned} p_s^i &= E_{r,I_{ei}}\left(P\left(\max_{e\in\theta_e} \mathrm{SNR}_e^i > 2^{R_e} - 1\right)\right) \\ &= E_{r,I_{ei}}\left(1 - \prod_{e\in\theta_e} P(\mathrm{SNR}_e^i < 2^{R_e} - 1)\right) \\ &= 1 - E_{r,I_{ei}}\left(\prod_{e\in\theta_e} P\left(|\hat{h}_{ie}^H h_{\hat{l}}|^2 < \frac{(2^{R_e}-1)(I_{ei}+\sigma_e^2)}{P_i |Y_{ie}|^{-\alpha_i}}\right)\right), \end{aligned} \tag{18}$$

which is not easy to get the directly result. Since we derive the upper and lower bound to approximate the secrecy outage probability.

Lemma 3. The upper bound of SOP is derived as follows:

$$p_{s,\mathrm{upper}}^i = 1 - \exp\left(-\pi\lambda_e \int_0^\infty \exp\left(-\frac{(2^{R_e}-1)\sigma_e^2}{P_i |r|^{-\alpha_i}} - \pi \sum_{j=1}^K \lambda_j 1/\alpha_j (k_2 P_j)^{2/\alpha_j} \Theta\right) \mathrm{d}r\right), \tag{19}$$

which $\Theta = \sum_{k=1}^{N_j} B(1 - 2/\alpha_j, k + 2/\alpha_j - 1)$.

And the lower bound can be defined as the nearest Eve to the BS. Therefore the lower bound can be expressed as follows:

$$p_{s,\mathrm{lower}}^i = \int_0^\infty 2\pi\lambda \exp\left(-\frac{(2^{R_e}-1)\sigma_e^2}{P_i |r|^{-\alpha_i}} - \pi \sum_{j=1}^K \lambda_j 1/\alpha_j (k_2 P_j)^{2/\alpha_j} \Theta\right) - \pi\lambda_e r^2 \mathrm{d}r. \tag{20}$$

According to [20], when $\lambda_e \ll 1$, the approximate result is express as

$$p_s^i \approx \int_0^\infty 2\pi\lambda_e \exp\left(-\frac{(2^{R_e}-1)\sigma_e^2}{P_i |r|^{-\alpha_i}} - \pi \sum_{j=1}^K \lambda_j 1/\alpha_j (k_2 P_j)^{2/\alpha_j} \sum_{k=1}^{N_j} \Theta\right) \mathrm{d}r. \tag{21}$$

Proof. The proof is given in Appendix C.

Property 4. The p_s^i is decreasing with R_e and P_j, while increasing with λ_e and P_i.

Similarly, Property 4 can be derived from partial derivatives of various system parameters. As the density of the Eve increases, the probability of its proximity to the BS increases correspondingly, causing the secrecy outage probability rises. At the same time, since the channel and the user's main channel are independent of each other, the private signal strength at Eve is only related to the transmission power of the transmitting BS, and is independent of the number of antennas. Further, when the power of other BSs increases, the probability happening secrecy outage tends to decrease, because of the increasing inter-layer interference.

4 Secrecy throughout maximization

In this section, we focus on the average secrecy throughput. We attribute this evaluation indicator to the tradeoff between feedback overhead and data transmission in a fixed coherent time. A large amount of channel feedback can improve the CSI quality, but reduce the time available for data transmission; while a small amount of feedback time leads to poor beamforming performance, which reduces the reachable confidentiality. Motivated by these facts, we are more concerned about designing coding parameters and feedback parameters in the determined system to maximize the system's secrecy throughput.

First, we define the average throughput of the target user as

$$\Omega = \sum_{i=1}^{K} \mathcal{A}_i \Omega_u^i. \tag{22}$$

The Ω_u^i represents the user's secrecy throughput when access to tier-i. Recalling the protocol designed in Section 2, the time belonging to feedback overhead is $T_{f,i} = 2^{B_i} I_c N_i + B_i / R_{\text{up}}$. The first part represents the time searching for the optima index in the codebook by exhaustive searching. It is related to the time cost for a complex multiplication I_c and the antenna number N_i. The second part is the feedback transmission time. When B_i is small, the second part will play the major role to influence the time overhead. On the opposite, the exponential growth of searching time will cost more when B_i is large. So we define the Ω_u^i as

$$\Omega_u^i = (R_b - R_e)(1 - p_s^i(R_e)) p_u^i(R_b)(T_c - T_{f,i}). \tag{23}$$

The optimization problem is formulated as

$$\max_{\boldsymbol{B}, R_b, R_e} \Omega \qquad \text{s.t. } 0 < T_{f,i} \leqslant T_c;\ p_c^i(R_b) > \kappa;\ p_{so}^i(R_e) < \varphi; \tag{24}$$

where $\boldsymbol{B} = \{B_1, B_2, \ldots, B_K\}$ is the feedback length in every tier. However, the feedback length and R_b, R_e have complex interaction, for example, and the feedback length will determine the bounds of the code rate and redundancy rate. The problem is intractable to solve directly. Such we divide the problem into two subproblems and utilize an iterative and mutual searching algorithm to handle it. In particularly, we first optimize the feedback length of each tier under the certain R_b, R_e, then search the optimal coding parameter with fixed $\boldsymbol{B}$. We present the subproblem and solutions in the following.

(1) The optimal $\boldsymbol{B}$ under fixed R_b, R_e. According to Property 1, the change of B_i has no influence on other tiers without artificial noise. So we can find the optimal feedback length tier by tier. The sub-problem is changed into

$$\max_{B_i} \Omega_u^i \qquad \text{s.t. } 0 < T_{f,i} \leqslant T_c. \tag{25}$$

For each tier, we can take the first order derivative of Ω_i on B_i as

$$\frac{\partial \Omega_u^i}{\partial B_i} = (R_b - R_e)(1 - p_s^i(R_e)) \left(\frac{p_u^i(R_b)}{\partial B_i} (T_c - T_{f,i}) - p_u^i(R_b) \frac{T_{f,i}}{\partial B_i} \right), \tag{26}$$

which $\frac{p_u^i(R_b)}{\partial B_i} = 2^{B_i}\ln 2\mathrm{e}^{-\lambda}F_\Gamma(\frac{\varepsilon\lambda}{1-\varepsilon})$ is always positive for any B_i. We can easily find that when $B_i \to 0$ the derivative appears positive and when $B_i \to B_{i,\max}$ becomes negative. Because there must be at least one zero point between 0 to $B_{i,\max}$.

We can see that the sub-problem is a typical nonlinear programming problem, which is difficult to solve the problem by an equation. Some proposed solutions can solve similar problems more effectively [16,17]. The most used heuristic search algorithm is the explicit enumeration method (EEM). Different from the conventional heuristic search algorithm, the EEM algorithm can find an optimal solution effectively in a small scale, and the complexity has advantages with the global search. Fortunately, we find that the sub-problem is quite suitable for using the EEM. The sub-algorithm is described as Algorithm 1.

Algorithm 1 Sub-algorithm for solving problem (25)

Input: Current R_b and R_e;
Initial $B_{i,\max}$, $\Omega^i_{\text{opt}} = 0$, $B_{i,\text{opt}} = 1$;
for $B_i = 1, 2, \ldots, B_{i,\max}$ **do**
  Compute Ω^i_u using Eq. (25);
  if $\Omega^i_u > \Omega^i_{\text{opt}}$ **then**
    update $\Omega^i_{\text{opt}} = \Omega^i_u, B_{i,\text{opt}} = B_i$;
  end if
end for
Output: Optimal $B_{i,\text{opt}}$.

(2) The optimal R_b and R_e with fixed $\boldsymbol{B}$. Based on above analysis, there is a complex interaction between the optimal coding rate and the optimal feedback length, which greatly improves the difficulty of solving the optimal problem. For this sub-question, after determining the feedback length of each layer through Algorithm 1, the problem 1 is equivalent to

$$\max_{R_b,R_e} \Omega \qquad \text{s.t. } p_c^i(R_b) > \kappa;\ p_{so}^i(R_e) < \varphi. \tag{27}$$

According to Properties 1 and 5, with the increase of R_b and R_e, the coverage probability and the secrecy outage probability decrease. Under the condition of coverage constrain κ and secrecy outage constrain φ, the maximum code rate $R_{b,\max}$ and minimum redundancy rate $R_{e,\max}$ can be obtained by solving the transcendental equation. While we can obtain a more simple form in the limited-interference scenario with $\alpha = 4$:

$$R_{e,\min} = \log_2\left(1 + \frac{\varphi\sum_{i=1}^K \mathcal{A}_i\lambda_j(\frac{P_j}{P_i})^{1/2}\Theta_j}{2\sqrt{\pi}\lambda_e}\right), \tag{28}$$

where $\Theta_j = \sum_{k=1}^{N_j} B(1-1/2, k-1/2)$. According to the definition of the throughput, the R_e must lower than the code rate R_b. By taking the first-order derivative of Ω on R_e, we derive $\frac{\partial\Omega}{\partial R_e}$ as

$$\frac{\partial\Omega}{\partial R_e} = -\sum_{i=1}^K \mathcal{A}_i p_u^i(R_b)(1-\zeta J(R_e)), \tag{29}$$

where $\zeta = \frac{\sum_{j=1}^K \lambda_j(\frac{P_j}{P_i})^{1/2}\Theta_j}{4\lambda_e\sqrt{\pi}}$ and $J(R_e)$ is given by

$$J(R_e) = \frac{1}{(2^{R_e}-1)^{1/2}}\left(1 + \frac{\ln 2}{2}\frac{2^{R_e}(R_b - R_e)}{(2^{R_e}-1)}\right). \tag{30}$$

It is easy to figure out that $J(R_e)$ is positive for $R_e \in (0, R_b)$, and it is a decreasing function of R_e between 0 and R_b. When $R_e \to 0$, $J(R_e) \to \infty$ and when $R_e \to R_b$, $J(R_b) \to (2^{R_b}-1)^{-1/2}$. Finally the result of $\zeta J(R_b)$ is equal to the secrecy outage probability $p_{so}^i(R_b)$ which is smaller than 1. In summary, the throughput $\frac{\partial\Omega}{\partial R_e}$ is bigger than 0 when $R_e \to 0$ and smaller than 0 when $R_e \to R_b$. In the same time, it is the decreasing function of R_e. So there is a maximization value between 0 and R_b. Based above discussion, we can present the optimal R_e in Theorem 1.

Theorem 1. For a fixed R_b, the optimal R_e maximizing the average secrecy throughput is

$$R^*_{e,\text{opt}} = \begin{cases} R_{e,\min}, R_{e,\min} > R_{e,\text{opt}}; \\ R_{e,\text{opt}}, R_{e,\min} < R_{e,\text{opt}} < R_b, \end{cases} \tag{31}$$

which $R_{e,\text{opt}}$ satisfies

$$\sum_{i=1}^{K} \mathcal{A}_i p_u^i(R_b)(1 - \zeta J(R_{e,\text{opt}})) = 0. \tag{32}$$

Although we cannot derive the explicit formula of the $R_{e,\text{opt}}$, but we can effectively calculate it through the binary search method. Similarly, $R_{b,\max}$ is hard to get the exact result because of the hypergeometric functions in (13). Fortunately, the p_c^i is the monotonically decreasing function of R_b. We can effectively calculate $R_{b,\max}$ that satisfies the $p_c^i(R_{b,\max}) = \kappa$ even the $R_{b,\text{opt}}$ using the traversing search algorithm.

So far, the optimal problem is transformed into two sub-problems, which is familiar with [27,28]. First the system parameters are initialized in step 0. Then in step n, we calculate the optimal $\boldsymbol{B}[n]$ for a given $R_b[n-1]$ and $R_e[n-1]$, then use the traversing search algorithm to find the optimal $R_b[n]$ and $R_e[n]$ under $\boldsymbol{B}[n]$. Repeating this process until the improvement of average secrecy throughput is smaller than the precision threshold. So an iterative algorithm to calculate the optimal parameter is shown in Algorithm 2.

Algorithm 2 Iterative algorithm for solving the problem (24)

Initial $\Delta R_\text{b} > 0$, $\varepsilon > 0$, $\Omega_\text{opt} = 0$, $R_b[0] = 2$, $R_e[0] = 1$, $\boldsymbol{B}[0] = \{1, \ldots, 1\}$, $n = 1$;
while $\Omega(\boldsymbol{B}[n], R_b[n], R_e[n]) - \Omega(\boldsymbol{B}[n-1], R_b[n-1], R_e[n-1]) > \varepsilon$ **do**
  $n = n + 1$;
  Find $\boldsymbol{B}[n]$ using sub-algorithm for each tier;
  while $R_b = R_b + \Delta R_b$ and $p_c^i(R_b) > \kappa$ **do**
    Get the R_e by solving (31);
    Calculate Ω using (22);
    if $\Omega > \Omega_\text{opt}$ **then**
      Update $\Omega_\text{opt} = \Omega$, $B_{i,\text{opt}} = B_i$, $R_{b,\text{opt}} = R_b$, $R_{e,\text{opt}} = R_e$;
    end if
  end while
end while
Output: Optimal $\boldsymbol{B}[n], R_b[n], R_e[n]$.

ΔR_b represents the accuracy requirement when solving the coding parameters. As indicated in [18], this two-step iterative algorithm can effectively reach the local optimum of the problem. We show the distance between the optimum result with the fixed feedback length scheme in Section 5.

5 Numerical results

In this section, we present some simulation results of the security performance of 2-tier HCN with limited feedback. Considering the typical HCN parameters, where the density is set as $\lambda_1 = \frac{1}{\pi 400^2 m^2}$ and $\{\lambda_2, \lambda_u, \lambda_e\} = \{4, 10, 5\}\lambda_1$, the transmit power is $\{P_1, P_2\} = \{30, 10\}$ dBm. In particular, we set passing loss $\alpha = 4$ and estimation error $\sigma_m^2 = 0.1$. Unless otherwise specified, we set $\{B_1, B_2\} = \{6, 4\}$ and the transmit antenna is $\{N_1, N_2\} = \{8, 4\}$.

Figure 3 plots the average coverage probability of tier-1 and tier-2 vs. B_1 with different antenna numbers, which includes theoretical analysis and the simulation result. The Monte-Carlo simulation is getting over 10000 times channel realization and corroborate the theoretical result. We did not calculate when B_1 is larger than 20 because of the ultra-high searching complexity. We can see that when B_1 is very small (for example $B_1 = 2$), the coverage probabilities for different antenna numbers do not have memorable difference. While if the feedback length is larger than the antenna number, the difference is more sizeable. When N_1 becomes larger, the performance gain obtained by adding antenna is small which

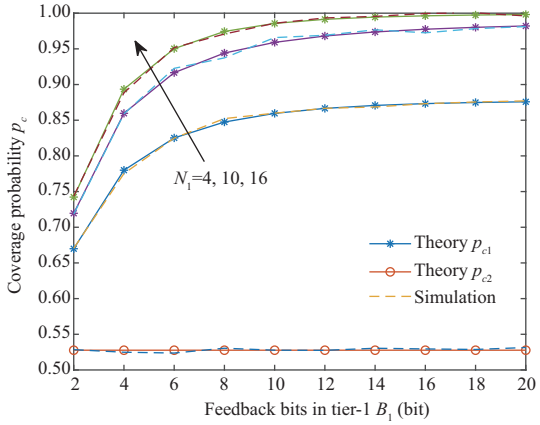

Figure 3 (Color online) Coverage probability in a 2 tier HCN vs. feedback length in tier-1 B_1.

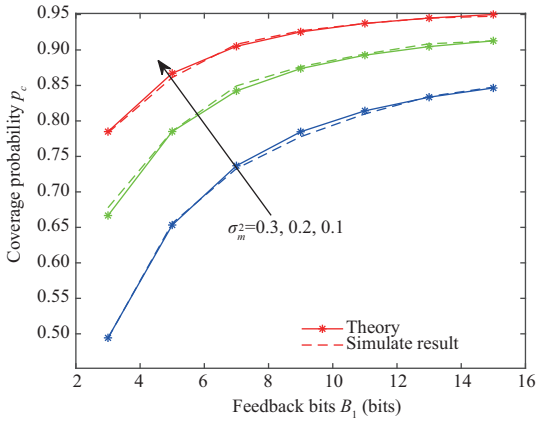

Figure 4 (Color online) Coverage probability in a 2 tier HCN vs. different estimation error σ_m^2.

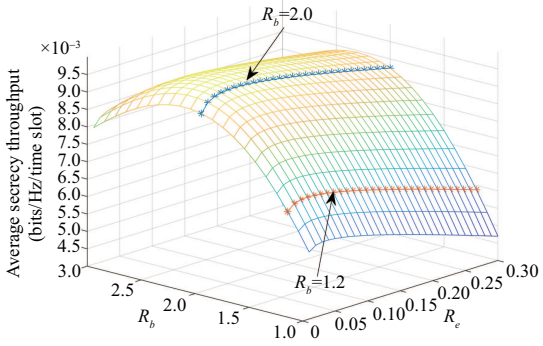

Figure 5 (Color online) The secrecy throughput vs. R_b and R_e.

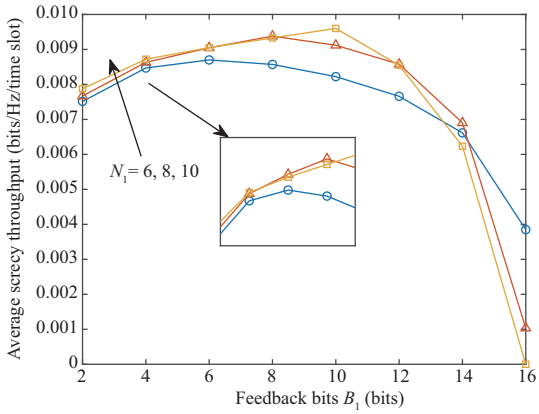

Figure 6 (Color online) The max average secrecy throughput vs. different feedback lengths.

shown by the comparison of N_1 with 4, 10 and 10, 16. What's more, although the growth of antenna number will cause larger CSI error after feedback, it is also beneficial for users' connect performance.

Figure 4 shows that the influence of the feedback length under different estimation errors. Different from Figure 1, the coverage performance when feedback length is small becomes significant different. And when B_1 increases, there is an upper bound of coverage probability. This is because that the feedback CSI is quantized result after channel estimation. When estimation error is large, the quantized CSI is only close to the estimation CSI but cannot approximate the real CSI. The simulation result proves the Property 3.

As illustrated in Figure 5, the average secrecy throughput increases first and then decreases with R_b and R_e which is consistent with the previous analysis. We can analyze more intuitively that when R_b is small, although the coverage probability is large, the multiplication is small; when R_b is large, the coverage will drop very seriously, making the system throughput approach to 0, which is same as the analysis of R_e. Although the code rate has the maximum point, the constrain of the coverage and secrecy outage probability limits the variation range of R_b and R_e. The AST under the constrain is shown below.

Figure 6 shows the trend of the average secrecy throughput of the target user. We should explain that the throughput is small because we just consider throughput per time slot (10 ms). When the feedback is small enough, the max average secrecy throughput have few growth within the antenna number. And the system with more antennas maybe not better than the less one. With the development of feedback length, the AST first increases and then decreases to 0. When B_1 comes to $B_{1,\max}$, the throughput fall

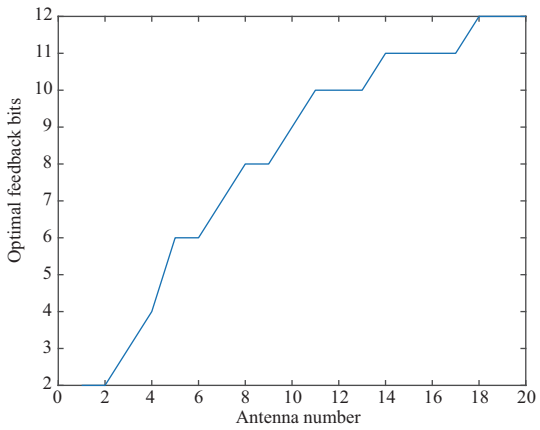

Figure 7 (Color online) The optimal feedback length vs. antenna numbers.

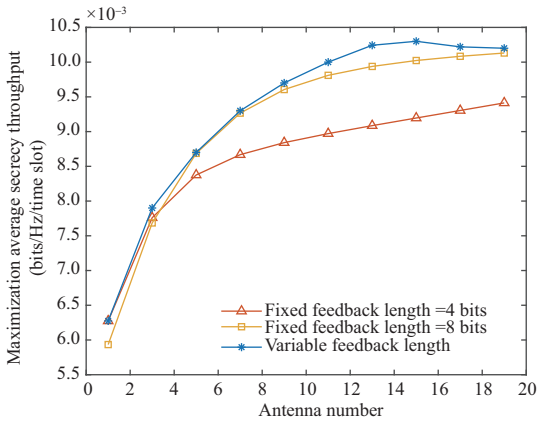

Figure 8 (Color online) Maximization average secrecy throughput vs. antenna numbers.

to 0 quickly, and the number of antenna is even harmful to the AST. The reason is that the antenna number have influences on the codebook searching time, which make the transmission time drop to 0. What's more, we can see that the optimal feedback length is different between different antenna numbers, which confirm our suspect. Therefore, we derive the optimal feedback and maximization throughput with different antenna numbers in Figure 7.

In Figure 7, the optimal feedback length grows as the antenna number increases. However, when the antenna is few (e.g., antenna number < 8), the optimal feedback length and max throughput grow in a linear form. While the feedback length gradually grows slow when the number is large. In Figure 8, two fixed feedback strategies are compared with the variable feedback strategy. It is obvious that the variable feedback length has more reliability. What's more, when the number of antenna rises, the searching time will serious impact the efficiency of the system. In summary, the feedback transmission has a major influence when feedback length is few, while the searching time has greater influence when feedback length is large. Furthermore, the optimal feedback length becomes instant, the increased antenna will spend more time to transmit data, make the throughput become lower. That is, it is not as many antennas as possible that have benefit for the cellular network within a coherent time.

6 Conclusion

In this paper, we designed the secure transmission protocol of HCNs with limited feedback. Applying the variety of feedback length and PLS key generation, the protocol can help the BS get more accurate and secure CSI without channel reciprocity. The coverage probability and secrecy outage probability provide the insights into the associated parameter such as antenna number and feedback length. At last, we proposed an algorithm to maximize the average secrecy throughput with coverage and secrecy outage constrain. The numeric results verify the property and security of the system. Possible future extensions include proposing a more efficient way to protect the uplink feedback security, and compare the secrecy performance with artificial noise aided secure transmission scheme.

Acknowledgements This work was supported in part by National Key Research and Development Program of China (Grant No. 2017YFB0801900).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Ghosh A, Mangalvedhe N, Ratasuk R, et al. Heterogeneous cellular networks: from theory to practice. IEEE Commun Mag, 2012, 50: 54–64
2 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
3 Mukherjee A, Fakoorian S A, Huang J, et al. Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun Surv Tut, 2014, 16: 1550–1573
4 Fan L S, Yang N, Duong T Q, et al. Exploiting direct links for physical layer security in multiuser multirelay networks. IEEE Trans Wirel Commun, 2016, 15: 3856–3867
5 Chen X, Chen H H. Physical layer security in multi-cell MISO downlinks with incomplete CSI-A unified secrecy performance analysis. IEEE Trans Signal Process, 2014, 62: 6286–6297
6 Shin W, Vaezi M, Lee B, et al. Non-orthogonal multiple access in multi-cell networks: theory, performance, and practical challenges. IEEE Commun Mag, 2017, 55: 176–183
7 Haenggi M, Andrews J G, Baccelli F, et al. Stochastic geometry and random graphs for the analysis and design of wireless networks. IEEE J Sel Areas Commun, 2009, 27: 1029–1046
8 Pinto P C, Barros J, Win M Z. Physical-layer security in stochastic wireless networks. In: Proceedings of the 11th IEEE Singapore International Conference on Communication Systems, 2008. 974–979
9 Zheng T X, Wang H M, Yin Q. On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers. IEEE Commun Lett, 2014, 18: 1299–1302
10 Ghogho M, Swami A. Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers. In: Proceedings of IEEE International Conference on Communications Workshops (ICC), 2011
11 ElSawy H, Hossain E, Haenggi M. Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: a survey. IEEE Commun Surv Tut, 2013, 15: 996–1019
12 Wang H, Zhou X Y, Reed M C. Physical layer security in cellular networks: a stochastic geometry approach. IEEE Trans Wirel Commun, 2013, 12: 2776–2787
13 Zhong Z H, Peng J H, Luo W Y, et al. A tractable approach to analyzing the physical-layer security in K-tier heterogeneous cellular networks. China Commun, 2015, 12: 166–173
14 Geraci G, Dhillon H S, Andrews J G, et al. Physical layer security in downlink multi-antenna cellular networks. IEEE Trans Commun, 2014, 62: 2006–2021
15 Love D J, Heath R W, Santipach W, et al. What is the value of limited feedback for MIMO channels? IEEE Commun Mag, 2004, 42: 54–59
16 Zhang X, Zhou X Y, McKay M R, et al. Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2014. 3968–3972
17 Zhang X, McKay M R, Zhou X Y, et al. Artificial-noise-aided secure multi-antenna transmission with limited feedback. IEEE Trans Wirel Commun, 2015, 14: 2742–2754
18 Hu J W, Cai Y M, Yang N, et al. Artificial-noise-aided secure transmission scheme with limited training and feedback overhead. IEEE Trans Wirel Commun, 2017, 16: 193–205
19 Wang H M, Wang C, Ng D W. Artificial noise assisted secure transmission under training and feedback. IEEE Trans Signal Process, 2015, 63: 6285–6298
20 Wang H M, Zheng T X, Yuan J, et al. Physical layer security in heterogeneous cellular networks. IEEE Trans Commun, 2016, 64: 1204–1219
21 Santipach W, Honig M L. Capacity of a multiple-antenna fading channel with a quantized precoding matrix. IEEE Trans Inform Theory, 2009, 55: 1218–1234
22 Zhou S L, Wang Z D, Giannakis G B. Quantifying the power loss when transmit beamforming relies on finite-rate feedback. IEEE Trans Wirel Commun, 2005, 4: 1948–1957
23 Li G Y, Sun C, Zhang J Q, et al. Physical layer key generation in 5G and beyond wireless communications: challenges and opportunities. Entropy, 2019, 21: 497
24 Li G Y, Hu A Q, Sun C, et al. Constructing reciprocal channel coefficients for secret key generation in FDD systems. IEEE Commun Lett, 2018, 22: 2487–2490
25 Gradtejn I S, Ryik I M, Jeffrey A. Table of Integrals, Series, and Products. Amsterdam: Elsevier, 1980
26 Xia P, Chandrasekhar V, Andrews J G. Open vs. closed access femtocells in the uplink. IEEE Trans Wirel Commun, 2010, 9: 3798–3809
27 Qi X H, Huang K Z, Li B, et al. Physical layer security in multi-antenna cognitive heterogeneous cellular networks: a unified secrecy performance analysis. Sci China Inf Sci, 2018, 61: 022310
28 Chu Z, Cumanan K, Ding Z G, et al. Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer. IEEE Trans Veh Technol, 2015, 64: 1833–1847