Beamforming Design for Physical Layer Security and Energy Efficiency Based on Base Station Cooperation

Wei Zhao(✉), Hao Zhang, Hui Bao, and Baogang Li

Department of Electronic and Communication Engineering,
North China Electric Power University (NCEPU), Baoding, China
andyzhaoster@gmail.com, winnerzh1991@163.com,
baohui20131228@126.com, baogangli@ncepu.edu.cn

Abstract. The balance problem between physical layer security and energy efficiency of legitimate users is jointly considered in this paper. After using the cooperation technology of macrocell base station and microcell base station as well as the derivation of convex optimization theory, we propose a cooperative beamforming scheme. From the perspective of secrecy energy efficiency and SINR, the simulation results show that the proposed algorithm can meet the requirements of the system security and energy efficiency.

Keywords: Physical layer security · Energy efficiency · Beamforming
Base station cooperation

1 Introduction

The rapid development of wireless communication makes the mobile communication users not only put forward higher requirements on the system security rate, but also request more harsh conditions for the energy consumption of the system. How to improve the energy efficiency while ensuring the physical layer security of is a hot issue in the field of wireless communication. As one of the key technologies in LTE-A, the base station cooperation technologyis an effective means to solve the aboveproblem [1–3]. This paper is organized as follows. In Sect. 2, we summarize the technology of base station cooperation in heterogeneous networks (HetNet). The system model in the downlink HetNet is proposed in Sect. 3, in which we introduce the user distribution in two-layer HetNet in detail. More importantly, the optimization algorithm is designed about the collaboration between multiple base stationsin Sect. 4 and simulation results

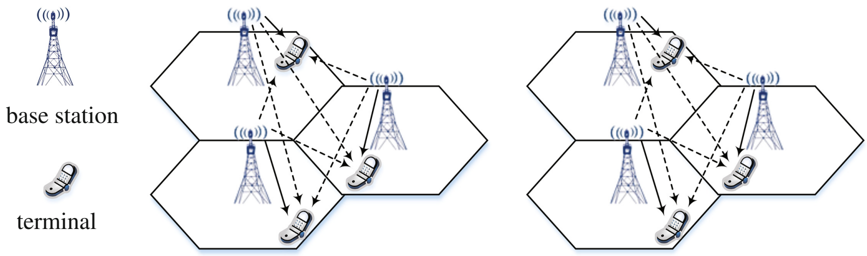
This work was supported by Beijing Natural Science Foundation (Grants No. 4164101), the Fundamental Research Funds for the Central Universities(Grants No. 2015MS95), National Natural Science Foundation of China (Grants No. 61501185), and Hebei Province Natural Science Foundation (Grants No. F2016502062).

K. Long et al. (Eds.): 5GWN 2017, LNICST 211, pp. 347–358, 2018.
https://doi.org/10.1007/978-3-319-72823-0_33

show the effectivenessof the proposed algorithms in Sect. 5. Finally, concluding remarks are provided in Sect. 6.

2 Overview of Base Station Cooperative Technology

The basic idea of cooperative technology is to use the base stations, antennas, relays, users and other communication nodes in the network to establish a virtual antenna array, and then get space diversity or multiplexing gain. Figure 1 shows a schematic diagram of a typical base station cooperative communication [4–6]. Different from the traditional collaboration techniques, the cooperation between base stations can fully utilize each antenna to carry out joint signal detection or data transmission on the same frequency resource block and transform the interference signal between multiple base stations into the useful one. The technology can achieve multi-point cooperative transmission at the station level and obtain diversity gain at the receiving node at the same time.



(a) The traditional collaboration techniques (b) The cooperative network

Fig. 1. Base station cooperative communication

Note: in (a), the solid line indicates the message signal, and the broken line indicates the interference; in (b), the solid line represents the message signal, and the dashed line represents the available signal transmitted by the cooperative base station.

There are two main types of cooperative communication at the physical level: cooperative communication between different base stations and cooperative communication between base stations and terminals. One of the preconditions for base station collaboration is to exchange information and data between multiple cooperating base stations, which is one of the biggest problems for the traditional cellular network. However, under the LTE-Advanced standard, it's proposed that the base station can communicate with each other through the X2 interface, thus providing the possibility for the base station to cooperate.

The optimization of HetNet using base station collaboration technology has the following advantages:

(1) Increase capacity. In [7], the method of distributed compression is used to limit the uplink data rate of two users in HetNet with different backhaul rates. In this way, the cellular uplink capacity can greatly improve.
(2) Improve edge user performance. Since the user at the cell edge is farther from the central base station, the signal attenuation is more severe. It is possible to significantly improve the communication quality of the cell edge users by the space diversity gain caused by the cooperative transmission using a plurality of base stations [8].
(3) Saving energy. On the one hand, under the condition of a certain probability of outage, the transmission power of the system can be greatly reduced by the cooperative diversity transmission of multi-base stations [9]; on the other hand, by using the resource dynamic control strategy and the operational state switching policy between the base stations, the transfer between users can be realized, and thus achieve the purpose of energy-saving base station [10].

More importantly, the base station collaboration technology is not only applied to the inter-user performance improvement, but also be used to address the needs of energy saving. For instance, I. Ashraf et al. proposed a cooperative technology of different base stations to reduce the energy consumption of the system in the overlapping coverage area of the network [11].

It is worth mentioning that most of the research focused on the base station in the homogeneous network collaboration or only using the base station collaboration technology to implement the physical layer security or energy efficiency. Applying base station collaboration technology into HetNet is rarely studied, which is a big waste of system resources.

In order to make full use of the characteristics of HetNet, this paper designs a collaborative beamforming scheme in the two-layer HetNet by using the collaboration between the macro base station and the micro base station. What's more, the intentionally introduced CCI (co-channel interference) is employed. The security rate of the legitimate users in the micro-cell is combined with the system energy efficiency and the convex optimization theory is used to derive the algorithm. Finally, a power allocation scheme is obtained. The simulation results show the advantages of the proposed algorithm in improving system security and reducing energy consumption from the two aspects of security energy efficiency and SINR (the ratio of the power of the message signal to the interference power plus the noise power).

3 System Model

In the downlink of HetNet, there is one macrocell base station equipped with $N_M (N_M > M)$ antennas, which locates at the center of its coverage, and K microcell base stations equipped with $\mathrm{N_P} (\mathrm{N_P} > \mathrm{N})$ antennas. For the sake of convenience, it is assumed that the macrocell base station and the microcell base station all have a circular area as shown in the following figure. The number of legal users in macrocell and microcell are all single antenna users and each macro cell can cover M number of legitimate users, while the number of legitimate users can be N. A single antenna eavesdropper is within the coverage of the macrocelland attempts to eavesdrop on the $n(1 \leq n \leq \mathrm{N})$ microcell user located in the $k(1 \leq k \leq \mathrm{K})$ microcell. Assume that all channels are independent of each other and subject to Rayleigh flat fading. Figure 2 is the multi-cell system model diagram of HetNet in this paper.

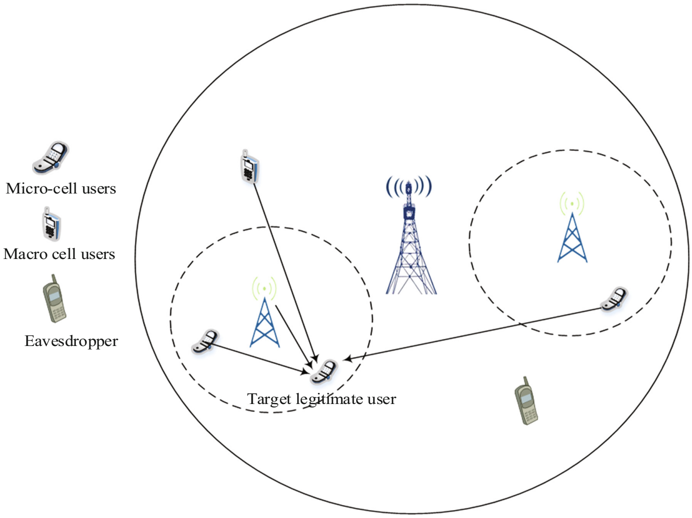


Fig. 2. System model

4 Optimization Algorithm Design

As can be seen from Fig. 2, the n-th legitimate user in the k-th microcell is listed as the reference object. Therefore, the desired message signal comes from the micro base station in the k-th microcell and the source of the interference includes other $N-1$ legitimate micro-cell users in the same microcell with the target legitimate user, all $(k-1) \cdot N$ legal microcell users in other $k-1$ microcells, M legitimate macrocell users and eavesdropper in the macrocell. It is assumed that both the macro base station and the micro base station can obtain a complete CSI.

Suppose there are $\mathrm{K}'(1 \leq \mathrm{K}' \leq K-1)$ cooperative microcell base stations can use CCI to interfere the eavesdroppers. Then according to the knowledge of information theory, the received signal of the target legitimate user can be expressed as:

$$y_{kn} = \underbrace{\mathbf{h}_{k,kn}\mathbf{w}_{kn}s_{kn}}_{\text{Useful signal}} + \underbrace{\sum_{\substack{a=1\\a\neq n}}^{N} \mathbf{h}_{k,kn}\mathbf{w}_{ka}s_{ka}}_{\substack{\text{Interference signals of other}\\ \text{n}-1\text{ users under the same microcell}}} + \underbrace{\sum_{\substack{b=1\\b\neq k}}^{K}\sum_{c=1}^{N} \mathbf{h}_{b,kn}\mathbf{w}_{bc}s_{bc}}_{\substack{\text{Interference from all }(\text{k}-1)\cdot\text{n}\\ \text{micro}-\text{cell users under all other k}-1\text{microcells}}} + \underbrace{\sum_{m=1}^{M} \mathbf{h}_{kn}\mathbf{w}_{m}s_{m} + n_{kn}}_{\substack{\text{Interference from all}\\ \text{M macrocell users}}} \quad (1)$$

Now the meaning of the variables in the formula is explained as follows:

Variable	Definition
$\mathbf{h}_{k,kn}$	The channel vector from the k-th microcell base station to the target legitimate user
$\mathbf{w}_{kn}$	The beamforming vector for the target legitimate user
s_{kn}	The message signal intended for the target legitimate user; The essence of s_{kn} is a normalized vector, Satisfying $E\left(\|s_{kn}\|^2\right) = 1$
$\mathbf{w}_{ka}$	The beamforming vector for other $n-1$ legitimate microcell users in the k-th microcell
s_{ka}	The message signal intended from the k-th microcell base station to other $n-1$ legitimate microcell users in the k-th microcell
$\mathbf{h}_{b,kn}$	The channel vector from other $k-1$ microcell base stations to the target legitimate user, $b \neq k$
$\mathbf{w}_{bc}$	The beamforming vector from other $k-1$ microcell base stations to the legitimate microcell users inside
s_{bc}	The message signal intended from other $k-1$ microcell base stations to the legitimate microcell users inside
$\mathbf{h}_{kn}$	The channel vector from the macrocell base station to the target legitimate user
$\mathbf{w}_{m}$	The beamforming vector from the macrocell users to the target legitimate user
s_{m}	The message signal intended from the macrocell base station to the target legitimate user
n_{kn}	n_{kn} obeying i.i.d. $CN \sim (0, \sigma_M^2)$

Similarly, the received signal at the eavesdropper is:

$$y_E = \mathbf{h}_E \mathbf{w}_{kn} s_{kn} + \sum_{\substack{a=1 \\ a \neq n}}^{N} \mathbf{h}_{n,E} \mathbf{w}_{ka} s_{ka} + \sum_{\substack{b=1 \\ b \neq k}}^{K} \sum_{c=1}^{N} \mathbf{h}_{b,kE} \mathbf{w}_{bc} s_{bc} + \sum_{m=1}^{M} \mathbf{h}_E \mathbf{w}_m s_m + n_{kn} \quad (2)$$

Suppose the user's CSI is known, according to the definition of SINR, the SINR of the target legitimate user is:

$$\mathbf{SINR}_{kn} = \frac{\left|\mathbf{h}_{k,kn} \mathbf{w}_{kn}\right|^2}{\sum\limits_{\substack{a=1 \\ a \neq n}}^{N} \left|\mathbf{h}_{k,kn} \mathbf{w}_{ka}\right|^2 + \sum\limits_{\substack{b=1 \\ b \neq k}}^{K} \sum\limits_{a=1}^{N} \left|\mathbf{h}_{b,kn} \mathbf{w}_{ba}\right|^2 + \sum\limits_{m=1}^{M} \left|\mathbf{h}_{kn} \mathbf{w}_m\right|^2 + \sigma_{kn}^2} \quad (3)$$

The SINR of the eavesdropper is:

$$\mathbf{SINR}_{E} = \frac{\left|\mathbf{h}_{E} \mathbf{w}_{kn}\right|^2}{\sum\limits_{\substack{a=1 \\ a \neq n}}^{N} \left|\mathbf{h}_{n,E} \mathbf{w}_{ka}\right|^2 + \sum\limits_{\substack{b=1 \\ b \neq k}}^{K} \sum\limits_{a=1}^{N} \left|\mathbf{h}_{b,kE} \mathbf{w}_{ba}\right|^2 + \sum\limits_{m=1}^{M} \left|\mathbf{h}_{E} \mathbf{w}_m\right|^2 + \sigma_{E}^2} \quad (4)$$

Then, according to the definition of confidential capacity, the confidential capacity of the target legitimate user is:

$$\mathbf{C}_S = \mathbf{C}_{kn} - \mathbf{C}_E = B\log_2(1+\mathbf{SINR}_{kn}) - B\log_2(1+\mathbf{SINR}_E) \tag{5}$$

According to the definition of security energy efficiency [12], the confidential energy efficiency of the target legal user can be obtained as:

$$\mathbf{J}_\mathrm{S} = \frac{\mathbf{C}_\mathrm{S}}{\mathbf{P}+P_0} = \frac{B\log_2(1+\mathbf{SINR}_{kn}) - B\log_2(1+\mathbf{SINR}_E)}{\mathbf{P}+P_0} \tag{6}$$

In summary, the optimization problem of security energy-efficient beamforming can be summarizedas follows:

$$\max_{\substack{\{\mathbf{w}_m\}_{\mathrm{m=1'}}^{M} \\ \left\{\{\mathbf{w}_{kn}\}_{\mathrm{n=1}}^{N}\right\}_{k=1}^{K}}} \frac{log(1+\mathbf{SINR}_{kn}) - log(1+\mathbf{SINR}_E)}{\mathbf{P}+P_0} \tag{7}$$

$$s.t. \quad \sum_{m=1}^{M} \|\mathbf{w}_m\|^2 \le P_M, m \in [1, \mathrm{M}] \tag{8}$$

$$\sum_{n=1}^{N} \|\mathbf{w}_{kn}\|^2 \le P_P, n \in [1, \mathrm{N}] \tag{9}$$

$$\mathbf{SINR}_m \ge \gamma_m \tag{10}$$

$$\mathbf{SINR}_{kn} \ge \gamma_{kn} \tag{11}$$

Next, we study the base station power optimization part.

The power amplifier is an important device in wireless communication system, the output power of which affects the transmission distance, thus affecting the entire coverage of macrocell. At the same time the power amplifier not only occupy a large weight in the wireless network static energy consumption, but alsoplay an important role in wireless network dynamic energy consumption. Therefore, from the base station side, through a reasonable power allocation to adjust the transmit power of base stationcan reduce the energy efficiency of the whole system.

Now optimize base station energy consumption. From the above description, wo can obtain the energy consumption of the system:

$$\mathbf{P} = \frac{\mathbf{P}_M}{\eta_M} + \sum_{n=1}^{N} \frac{\mathbf{P}_P^n}{\eta_p} + P_C \tag{12}$$

where $\mathbf{P}_M, \mathbf{P}_p$ is the transmit power of the power amplifier on the macrocell base station and the microcell base station side respectively; η_M, η_p is the effectiveness of the power amplifier; P_C is the total fixed circuit loss of the entire system.

Taking the target legitimate user as an example, we can get the transmit power of the macro base station as:

$$\begin{aligned}\mathbf{P}_M &= \sum_{n=1}^{N}\sum_{k=1}^{K}(\mathbf{w}_m)^{\mathrm{H}}\mathrm{E}(|s_{kn}|^2)\mathbf{w}_m + \sum_{m=1}^{M}(\mathbf{w}_m)^{\mathrm{H}}\mathrm{E}(|s_{kn}|^2)\mathbf{w}_m \\ &= \sum_{n=1}^{N}\sum_{k=1}^{K}(\mathbf{w}_m)^{\mathrm{H}}\mathbf{w}_m + \sum_{m=1}^{M}(\mathbf{w}_m)^{\mathrm{H}}\mathbf{w}_m\end{aligned} \tag{13}$$

Similarly, the transmit power at the base station side is:

$$\mathbf{P}_P = \sum_{n=1}^{N}\sum_{k=1}^{K}(\mathbf{w}_{kn})^{\mathrm{H}}\mathbf{w}_{kn} \tag{14}$$

Through fractional programming, the above formula can be decomposed into the external part and the internal part. The external function can eventually be derived as:

$$\begin{aligned}&\max \quad \frac{1+G(\tau)}{1+\tau} \\ &s.t. \quad 0 \le \mathrm{t} \le \mathrm{Tr}(\mathbf{H}_1)\mathrm{P}_{\mathrm{Mmax}}\end{aligned} \tag{15}$$

It can be seen that an external function can be solved using a one-dimensional linear search method. Among them, $G(\tau)$ is the internal function and can be optimized based on SDP optimization algorithm. The concrete optimization method is as follows:

$$\max_{\substack{\{\mathbf{w}_m\}_{\mathrm{m}=1'}^{M} \\ \left\{\{\mathbf{w}_{kn}\}_{\mathrm{n}=1}^{N}\right\}_{k=1}^{K}}} \frac{Tr(\mathbf{H}_m\mathbf{W}_m)}{\sum_{m=1}^{M} Tr(\mathbf{H}_m\mathbf{W}_m) + \sum_{n=1}^{N}\sum_{k=1}^{K} Tr(\mathrm{H}_{n,m}\mathbf{W}_{kn})} \tag{16}$$

$$s.t. \quad \sum_{m=1}^{M} Tr(\mathbf{X}_m) \le P_{M\max}\zeta \tag{17}$$

$$\sum_{n=1}^{N}\sum_{k=1}^{K} Tr(\mathbf{X}_{kn}) \le P_{P\max}\zeta \tag{18}$$

$$Tr(\mathbf{H}_m\mathbf{W}_m) \ge \gamma_m \left(\sum_{\substack{q=1 \\ q \ne m}}^{M} Tr(\mathbf{H}_m\mathbf{X}_q) + \sum_{n=1}^{N}\sum_{k=1}^{K} Tr(\mathbf{H}_{n,m}\mathbf{X}_{kn}) + \zeta \right) \tag{19}$$

$$Tr(\mathbf{H}_{n,kn}\mathbf{X}_{kn}) \geq \gamma_{kn}\left(\sum_{\substack{t=1\\t\neq k}}^{K} Tr(\mathbf{H}_{n,kn}\mathbf{X}_{tn}) + \sum_{\substack{p=1\\p\neq n}}^{N}\sum_{t=1}^{K} Tr(\mathbf{H}_{p,kn}\mathbf{X}_{tp}) + \sum_{m=1}^{M} Tr(\mathbf{H}_{kn}\mathbf{X}_{m}) + \zeta\right) \tag{20}$$

$$Tr(\mathbf{H}_{E}\mathbf{X}_{1}) \leq \tau\left(\sum_{m=1}^{M} Tr(\mathbf{H}_{E}\mathbf{X}_{m}) + \sum_{n=1}^{N}\sum_{k=1}^{K} Tr(\mathbf{H}_{n,E}\mathbf{X}_{kn}) + \zeta\right) \tag{21}$$

Where $\mathrm{H} = \mathrm{h}^{\mathrm{H}}\mathrm{h}$, $\mathrm{W} = \mathrm{w}^{\mathrm{H}}\mathrm{w}$, $W_m = \frac{\mathbf{X}_m}{\zeta}$, $W_{kn} = \frac{\mathbf{X}_{kn}}{\zeta}$ and X is the default auxiliary variable.

The optimization steps of the proposed algorithm can be summarized as follows:

Convex optimization method based on SDP:
1.Initial value: according to the simulation situation, give $\mathrm{P}_{\mathrm{Mmax}}$, $\mathrm{P}_{\mathrm{Pmax}}$, γ_m and γ_{kn} an initial value;
2.Compute $\tau_{\max} = Tr(\mathrm{H}_1)\cdot \mathrm{P}_{\mathrm{Mmax}}$;
3. Get the optimal solution $G^*(\tau)$ by solving the internal SDP function, under $\tau_{\max}$;
4. In the $[1, \tau_{\max}]$ interval, after the one-dimensional linear search method to calculate the external function, we can get the optimal solution;
5.Through τ^* we can easily get (X_m^*, X_{kn}^*, ζ^*);
6. Based on $W_m = \frac{X_m}{\zeta}$, $W_{kn} = \frac{X_{kn}}{\zeta}$,the optimal solution of the beamforming vector W_m^* and W_{kn}^* can be obtained

5 Simulation Analysis

In the actual simulation, the number of antennas is defined as follows: the antennas in the macro base station is $N_M = 10$, in the micro base station is $\mathrm{N_P} = 4$, and in the macro cell is $M = 2$,

That is a legitimate users for macro cell, and an eavesdropping users. The number of legitimate microcell users in the microcell is $K = 1$, which is a microcell contains only one user. Otherwise, we also assuming that the number of the antenna in macrocell and in microcell, including the legitimate user and eavesdropping user is only one, and the channel of the system is Rayleigh fading channel. The simulation results are as follows (Fig. 3):

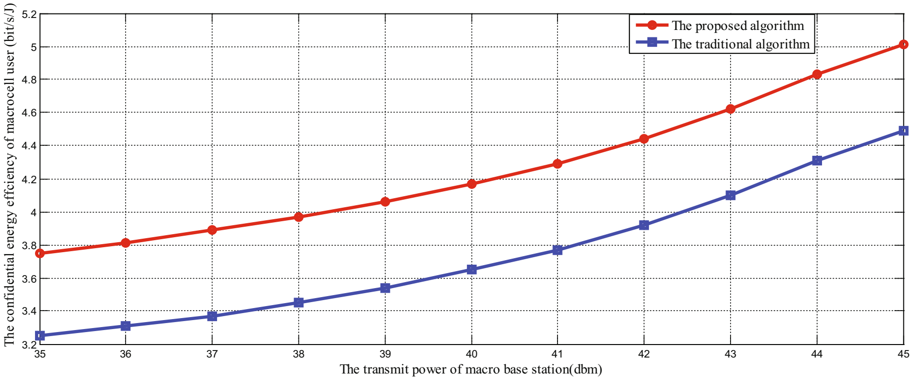


Fig. 3. The comparison of the traditional algorithm and the proposed algorithm on the security energy efficiency under different macro base station transmit power

The transmission power of the macro base station is not related to the cooperative interference between the micro base stations. However, according to the proposed algorithm, a significant improvement in security energy efficiency can be obtained (Fig. 4).

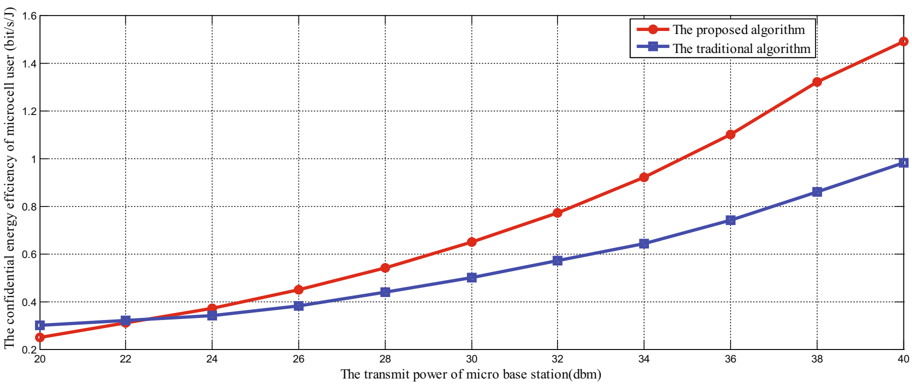


Fig. 4. The comparison of the traditional algorithm and the proposed algorithm on the security energy efficiency under different Micro base station transmit power

According to the simulation results, we can see that because of the cooperation between the micro base stations:

1. The transmission power is too small when the transmit power of micro-base station is less than 23 dbm, which leads to a large proportion of interference, therefore, it has a great influence on the security energy efficiency, so the proposed algorithm is slightly inferior to the traditional algorithm

2. The proposed algorithm is better than the traditional algorithm when the transmit power of micro-base station is exceed than 23 dbm. Because the transmitting power of the base station is increasing constantly, but the interference power is invariable, therefore, the curve is ascending.

Because of the presence of eavesdropping, the interference of the microcell increases larger than the legitimate signal along with the increase in transmission power at the macro base station, which causes the decreasing trend of SINR (Fig. 5).

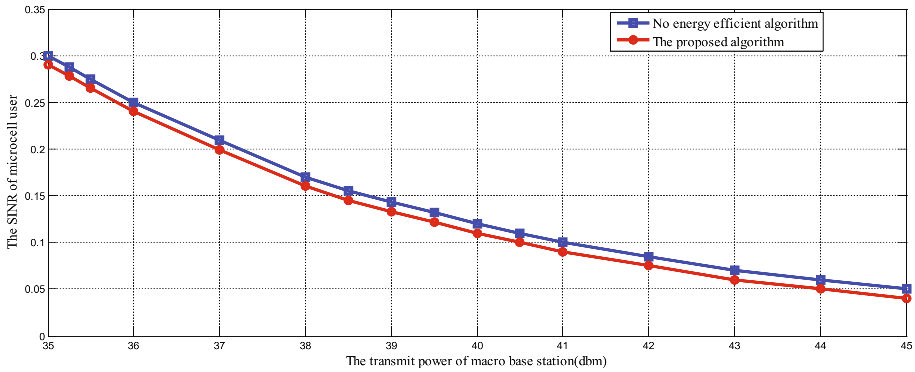


Fig. 5. Comparison of conventional algorithms and proposed algorithms in SINR at different transmit powers of the macro base station

Since the proposed algorithm is compromised optimization algorithm between energy-efficient and physical layer security, the resulting of beamforming vector W is smaller than the case where energy efficiency is not considered, therefore, the SINR is lower, but within an acceptable range (Fig. 6).

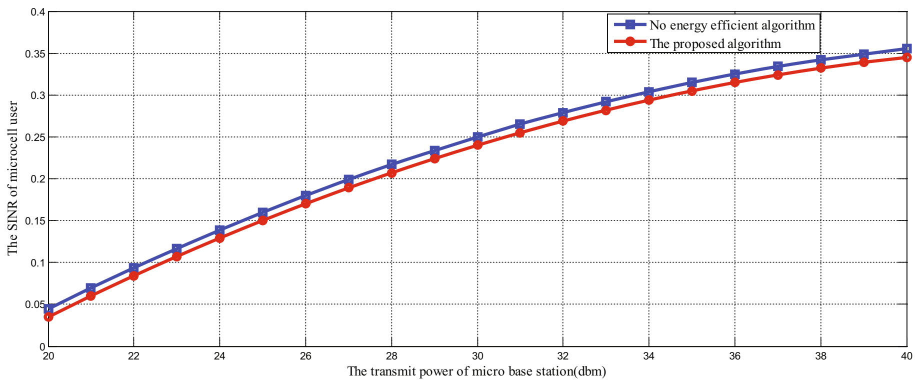


Fig. 6. Comparison of SINRs with traditional algorithms and proposed algorithms at different micro base station transmit powers

Different from the macro base station, the interference can be used as a means to interfering with the eavesdropping side. With the micro-base station transmission power increases, the SINR of micro-cell users also increases. But considering the energy efficiency and physical layer security, so the value is still slightly lower than the algorithm which the energy efficiency is not considered. Simultaneously, we also to know that with the cooperation of base stations between microcells and the effect of interference in microcell is larger than macrocell.

6 Concluding Remarks

This paper analyzes the tradeoff between physical layer security and energy efficiency of the legitimate users in HetNet. By using the CCI between cooperative micro-base stations, a cooperative beamforming scheme which conforms to the system model is designed; Combining the security rate of legitimate users in the microcell with the system energy efficiency, and using the convex optimization theory to derive the algorithm, a power allocation scheme is obtained. Finally, Simulation results show that, in the view of different macro base stations and micro-base station transmit power, a comparison chart between the traditional algorithm and the proposed algorithm is given. The results show that the proposed algorithm has the advantage of improving security and reducing energy consumption.

References

1. Zhang, H., Xing, H., Cheng, J., et al.: Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming. IEEE Trans. Industr. Inf. **12**(5), 1714–1725 (2016)
2. Zhao, J., Lu, Z., Wen, X., et al.: Resource management based on security satisfaction ratio with fairness-aware in two-way relay networks. Int. J. Distrib. Sens. Netw. **11**(7), 819195 (2015)
3. Zhang, H., Xing, H., Chu, X., et al.: Secure resource allocation for OFDMA two-way relay networks. In: 2012 IEEE Global Communications Conference (GLOBECOM), pp. 3649–3654. IEEE (2012)
4. Zhao, J., Zheng, W., Wen, X., Zhang, H., Lu, Z., Jing, W.: Research on the resource allocation of OFDMA relay network based on secrecy ratio. J. Electr. Inf. Technol. **36**(12), 2816–2821 (2014)
5. Zhang, H., Dong, Y., Cheng, J., et al.: Fronthauling for 5G LTE-U ultra dense cloud small cell networks. IEEE Wirel. Commun. **23**(6), 48–53 (2016)
6. Zhang, H., Liu, N., Chu, X., et al.: Network slicing based 5G and future mobile networks: mobility, resource management, and challenges. IEEE Commun. Mag. (2017)
7. Venturino, L., Prasad, N., Wang, X.: Coordinated scheduling and power allocation in downlink multicell OFDMA networks. IEEE Trans. Veh. Technol. **58**(6), 2835–2848 (2009)
8. Karakayali, M.K., Foschini, G.J., Valenzuela, R.A.: Network coordination for spectrally efficient communications in cellular systems. IEEE Wirel. Commun. **13**(4), 56–61 (2006)
9. Del Coso, A., Simoens, S.: Uplink rate region of a coordinated cellular network with distributed compression. In: 2008 IEEE International Symposium on Information Theory, pp. 2091–2095. IEEE (2008)

10. Jiang, C., Zhang, H., Ren, Y., et al.: Energy-efficient non-cooperative cognitive radio networks: micro, meso, and macro views. IEEE Commun. Mag. **52**(7), 14–20 (2014)
11. Shen, Y., Jiang, C., Quek, T.Q.S., et al.: Device-to-device cluster assisted downlink video sharing—a base station energy saving approach. In: 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP), pp. 108–112. IEEE (2014)
12. Liu, H., Zheng, W., Zhang, H., et al.: An iterative two-step algorithm for energy efficient resource allocation in multi-cell OFDMA networks. In: 2013 IEEE Wireless Communications and Networking Conference (WCNC), pp. 608–613. IEEE (2013)