Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 2753614, 7 pages
https://doi.org/10.1155/2018/2753614

Research Article

Physical Layer Security Performance Based on 3D Heterogeneous Network

Wei Zhao, Lingling Wu, Baogang Li, Hui Bao, and Chunxiu Zhang

School of Electrical and Electronic Engineering, North China Electric Power University, Hebei, Baoding 071000, China

Correspondence should be addressed to Wei Zhao; andyzhao@ncepu.edu.cn

Received 5 January 2018; Revised 21 March 2018; Accepted 18 April 2018; Published 24 May 2018

Academic Editor: Pierre-Martin Tardif

The distribution of the base stations (BSs) and users is mostly designed as a two-dimensional model in the study about heterogeneous networks (HetNets), which is not suitable for ultra-dense network scenarios. Meanwhile, the eavesdroppers existing in vertical dimension directly reduce the physical layer security of the HetNets. To tackle the mentioned problem, we propose to adjust the vertical dimension of the full-dimension (FD) antenna placed in the BSs; then the signal-to-noise ratios (SNRs) of the legitimate users and eavesdroppers are given due to the tilted angle. According to the three-dimensional Poisson point process (PPP) of BSs and users, the cumulative distribution function of SNR is deduced, which derives the closed expression of average security rate. The simulation results verify the correctness of the closed expression and the feasibility of proposed scenarios that the physical layer security performance can be improved by adjusting the vertical tilt angle. And density ratio of the BSs can be obtained in the various specific scenes.

1. Introduction

With the rapidly increasing number of wireless data capacity, the privacy and security of data transmission have great attention in wireless transmission. Wireless systems are more vulnerable due to the broadcast nature of wireless communications, which is solved by adding keys to the application layer in traditional research. Recently, the physical layer security technology can securely transmit information through the orthogonal characteristics of the physical layer resources [1]. The ultra-dense network is one of the key technologies in the fifth generation mobile communication systems, where the frequency utilization and coverage are improved [2]; with the deployment of ultra-dense networks, the coverage and improvement of the system throughput are the main fields in the research on its performance and transmission technologies. However, due to the high deployment density of ultra-dense network users and small-cell BSs and the fact that the channel openness characteristics have not changed, the research and optimization of physical layer security indicators in ultra-dense networks have caused great attention.

In the research of improving the physical layer security performance, the physical layer security performance is improved by transmitting artificial noise and optimizing the beamforming matrix [3–5]. In literature [6], the antenna selection method is proposed to improve the physical layer security performance of the HetNets. However, the above researches are all based on the network structure of two-dimensional random geometric distribution. At the same time, even if HetNets with large-scale antennas are researched, it is analyzed based on linear arrays. It can be seen that the above researches have ignored the effect of the eavesdropping user in vertical dimension.

Recently, the ultra-dense network is usually analyzed under the two-dimensional stochastic geometric distribution model, which is mainly applicable to rural areas or suburban areas, instead of the environment of urban centers with high distribution density [7]. In the central areas of the city, the distribution density of small-cell BSs and users is large, and most small-cell BSs and users are in the vertical dimension; in the traditional researches of the two-dimensional HetNets performance, the coverage rate [8], the system's outage

probability capacity [9], energy efficiency performance [10], and physical layer security performance [11] are researched; in literature [11], the security throughput of the users is derived in the D2D system. The method of artificial noise is applied in literature [7]; the connection probability and security probability of users are deduced by using stochastic geometry tools. In literature [12], the deployment density of small-cell BSs is optimized under the condition guaranteeing user service quality, which is proposed to optimize the energy efficiency of HetNets. In literature [13], the sleep probability and transmit power of the small-cell BSs are jointly optimized to minimize the energy consumption. The above research shows that the analysis of the ultra-dense network mostly focuses on transmission efficiency and energy utilization efficiency, where both the BSs and users follow the plane random geometric distribution. However, the literature [14] has shown that the HetNets models based on the plane random distribution can not accurately analyze the relative performance of HetNets. Three-dimensional random distribution originated in literature [15], where three-dimensional independent Poisson point distribution is applied to analyze the coverage of dense cellular HetNets. Compared with the coverage of the HetNets based on the plane random distribution, the coverage performance is more accurate. Large-scale fading, such as Floor Attenuation Factor (FAF), is researched in literature [16]; as a result, the coverage performance of the ultra-dense networks can be analyzed more accurately. In the literature [17], the secure connection probability of users is analyzed according to the three-dimensional MHCP distribution, and an optimal BSs sleeping mechanism is obtained to maximize energy efficiency. From the above research status, there are few researches on the analysis of ultra-dense network performance based on three-dimensional geometric distribution. And the physical layer security performance of the ultra-dense networks has not been researched.

In this paper, the small-cell BSs is equipped with full-dimension multiantenna, and the vertical dimension angle can dynamically be adjusted. We assume that the small-cell BSs and the user follow the three-dimensional PPP distribution; the closed expression of the system's security transmission rate is deduced. According to the performance of the security transmission rate, the optimal antenna down tilt angle and small-cell BSs distribution density are obtained. In future research, the secure beamforming algorithm is proposed for full-dimensional multiantennas to optimize the physical layer security performance of ultra-dense networks.

2. System Model

In this section, the small-cell BSs in HetNets are subject to PPP distribution Φ_p in three-dimensional space, where λ_p denotes the density. The macrocell BSs also follow the PPP distribution Φ_m with the density of λ_m. Also, the density of legitimate users is denoted by λ_s, while λ_e stands for the distribution density of the potential eavesdroppers. Due to the distribution of high-rise buildings in dense urban areas, the path attenuation factor is considered. The target legitimate user u is located at the origin, and other users are distributed in three-dimensional space. r denotes the distance between the BSs and the target user. Therefore, according to the Motley-Keenan path loss model in [1], the unit of the path loss is obtained as follows:

$$\mathrm{PL}(r) = \mathrm{PL}(r_0) + 10\alpha \log_{10}\left(\frac{r}{r_0}\right) + n_w \mathrm{WAF} + n_F \mathrm{FAF}, \quad (1)$$

where $\mathrm{PL}(r_0)$ denotes the path loss per unit length and $\mathrm{PL}(r_0 = 1m) = 40\,\mathrm{dB}$ when the frequency is 2.4 GHz. WAF and FAF are the average path loss for each wall and floor. n_w and n_F represent the number of walls and floors between transmitting and receiving antennas, respectively. WAF and FAF are chosen from 1 dB to 30 dB depending on the material of the walls and floors. According to various walls and floors, the Devasirvatham model in [11] can be introduced, and the model of path loss is rewritten:

$$\mathrm{PL}(r) = \mathrm{PL}(r_0) + 10\alpha \log_{10}\left(\frac{r}{r_0}\right) + \mathrm{AF}(r), \quad (2)$$

where $\mathrm{AF}(r)$ denotes the average impact factor of the wall and floor. The function expression of r is obtained by

$$\mathrm{AF}(r) = 10\log_{10}(\mu r), \quad (3)$$

where μ is the constant unit of the attenuation path. According to (3), the signal attenuation caused by path loss can be expressed as

$$Kr^{-(\alpha+1)}. \quad (4)$$

Here K is formulated as

$$K = \frac{r_0^{\alpha}}{\mu 10^{\mathrm{PL}(r_0)/10}}. \quad (5)$$

In this paper, the small-scale Rayleigh fading is considered, and users are served by the nearest small-cell BSs and macrocell BSs. The attenuation G of the vertical dimension is written by

$$G_{\mathrm{dB}}(\phi_{\mathrm{tilt}}) = -\min\left(12\left(\frac{\phi + \phi_{\mathrm{tilt}}}{\phi_{3\,\mathrm{dB}}}\right)^2, A_{\mathrm{dB}}\right), \quad (6)$$

where $\phi < 0$ is the acceptance angles of the BSs and users, $\phi_{\mathrm{tilt}} > 0$ denotes the tilt angle, $\phi_{3\,\mathrm{dB}}$ represents 3 dB beam width, and A_{dB} denotes the minimum leakage power outside the purpose district, of which the traditional value is 20 dB. Considering the omnidirectional antenna model in the horizontal plane, the angle ϕ can be expressed with the effective height H_{eff} (the height difference between the transmitting and receiving BSs) and a function of the distance R between the BSs and the users.

$$\phi = -\tan^{-1}\left(\frac{H_{\mathrm{eff}}}{R}\right). \quad (7)$$

Here, $H_{\mathrm{eff}} = H_a - H_{ue}$ denotes the effective height, which refers to the difference between the height H_{ue} and the height H_a of the BSs antenna. According to this definition, a linear expression is obtained by

$$G_{\mathrm{dB}}(R, \phi_{\mathrm{tilt}}) = 10^{-\min(12((-\tan^{-1}(H_{\mathrm{eff}}/R)+\phi_{\mathrm{tilt}})/\phi_{3\,\mathrm{dB}})^2, A_{\mathrm{dB}})/10}. \quad (8)$$

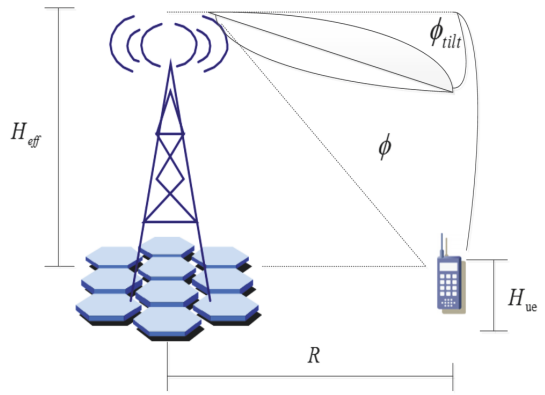

Figure 1: Geometric relationship among the various heights.

The geometric relationship among the heights is shown in Figure 1.

Any legitimate users are served by the nearest BS; as a result, the legitimate user not only receives the useful signal but also receives interference with other users and BSs. Then the SINR at the legitimate users receive is denoted by

$$\gamma_u = \frac{P_t \left\|h_{0,0}\right\|^2 K r^{-(\alpha+1)} G\left(r, \phi_{\text{tilt}}\right)}{I_p + I_m + \delta^2}, \tag{9}$$

where

$$\begin{aligned} I_p &= \sum_{i \in \Phi p \setminus \{0\}} P_t \left|h_{j,0}\right|^2 G\left(r_{j,0}, \phi_{\text{tilt}}\right) K d_i^{-(\alpha+1)}, \\ I_m &= \sum_{k \in \Phi m} P_m \left|g_{j,0}\right|^2 K l_j^{-(\alpha+1)}. \end{aligned} \tag{10}$$

P_t denotes the transmitted power of the small-cell BSs, P_m is the transmitted power of the macrocell BSs, and δ^2 denotes the noise power.

The cooperative mechanisms among eavesdroppers are not considered in this paper; as a result, we propose the security rate under the condition that the eavesdroppers get the minimum useful information. Any eavesdropper receives the signals from both legal users and the interference. Therefore, the received SINR at the eavesdroppers is obtained by

$$\gamma_e = \max_{e_k \in \Phi_e} \left\{ \frac{P_t \left|h_{0,e_k}\right|^2 K r_e^{-(\alpha+1)}}{I_{p,e} + I_{m,e} + \delta^2} \right\}, \tag{11}$$

where

$$\begin{aligned} I_{p,e} &= \sum_{i \in \Phi p \setminus \{0\}} P_t \left|h_{j,e_k}\right|^2 K d_i^{-(\alpha+1)}, \\ I_{m,e} &= \sum_{k \in \Phi m} P_m \left|g_{j,e_k}\right|^2 K l_j^{-(\alpha+1)}. \end{aligned} \tag{12}$$

3. Physical Layer Security Performance Analysis

The physical layer security performance is measured by the average security rate; then, the analytical expression of the average confidentiality rate is derived, and the overall average confidentiality rate is analyzed as well. Therefore, the instantaneous security rate for a legitimate user can be expressed as

$$C = \left[C_u - C_e\right]^+, \tag{13}$$

where $[x]^+ = \max\{x, 0\}$, $C_u = \log_2(1+\gamma_u)$ denotes the capacity between the BSs and the legal users, and $C_e = \log_2(1+\gamma_e)$ stands for the largest amount of mutual information of the eavesdropper.

Note that the estimation of the SINR at the legal users and eavesdroppers is the most important in (13); as a result, the cumulative distribution function of the SINR at the legitimate users and eavesdroppers is derived. Macrocell BSs and small-cell BSs are independent. Taking the distance r from the target legal users u to the nearest transmitting BSs into considered, that is, in the spherical space of radius R, the existence probability of the BSs is

$$P\{R < r\} = P\left\{\Phi\left(\frac{4}{3}\pi R^3\right) = 0\right\} = \exp\left(-\frac{4}{3}\pi\lambda R^3\right). \tag{14}$$

From the cumulative distribution probability in (14), the probability density function for $r > 0$ is denoted by

$$f(r) \approx 4\pi\lambda r^2 \exp\left(-\frac{4}{3}\pi\lambda r^3\right). \tag{15}$$

According to formula (9), the cumulative distribution function of SINR at the legal users is obtained as follows:

$$\begin{aligned} &F_{\gamma_u}(\gamma_u) \\ &= \int_0^\infty P\left\{\frac{P_t \left\|\mathbf{h}_{0,0}\right\|^2 G\left(r, \phi_{\text{tilt}}\right) K r^{-(\alpha+1)}}{I_p + I_m} < \gamma_u\right\} \\ &= \int_0^\infty P\left\{\left\|\mathbf{h}_{0,0}\right\|^2 < \varsigma\left(I_p + I_m\right)\right\} f(r)\, dr. \end{aligned} \tag{16}$$

Here, $\varsigma = \gamma_u P_t^{-1} G^{-1}(r, \phi_{\text{tilt}}) K^{-1} r^{(\alpha+1)}$ is a new definition.

By using the probability density functions of r and $\|\mathbf{h}_{0,0}\|^2$, formula (16) can be rewritten as follows:

$$\begin{aligned} F_{\gamma_u}(\gamma_u) = 1 - &\int_{r \geq 0} 4\pi r^2 \exp\left(-\frac{4}{3}\pi\lambda r^3\right) \\ &\cdot \int_{I_{p \geq 0}} \int_{I_{m \geq 0}} \exp(\sigma) f_p\left(I_p\right) \\ &\cdot f_m\left(I_m\right) dI_p dI_m dr, \end{aligned} \tag{17}$$

where $\sigma = -\varsigma(I_p + I_m + \delta^2)$. $f_p(I_p)$ and $f_m(I_m)$ are the probability density functions of I_p and I_m, respectively.

According to (17) and the definition of Laplace transform operator, it can be expressed as follows:

$$\begin{aligned} F_{\gamma_u}(\gamma_u) = 1 - \int_{r\geq 0} & 4\pi r^2 \exp\left(-\frac{4}{3}\pi\lambda_p r^3\right) \\ & \cdot \exp\left(-\gamma_u P_t^{-1} G^{-1}(r, \phi_{\text{tilt}}) K^{-1} r^{(\alpha+1)} \delta^2\right) \\ & \cdot L_{I_p}\left[-\gamma_u P_t^{-1} G^{-1}\left(r_{j,0}, \phi_{\text{tilt}}\right) K^{-1} r^{(\alpha+1)}\right] \\ & \cdot L_{I_m}\left[-\gamma_u P_t^{-1} K^{-1} r^{(\alpha+1)}\right] dr. \end{aligned} \tag{18}$$

Here, $L_{I_p}[\bullet]$ and $L_{I_m}[\bullet]$ are the Laplace transform operator of I_p and I_m, respectively. I_p and I_m are independent, and $s = \gamma_u P_t^{-1} K^{-1} r^{(\alpha+1)}$ is an equivalent variable; we can further derive the formula as follows:

$$\begin{aligned} L_{I_p} &= \mathrm{E}_{\{I_{\Phi_p}, |\mathbf{h}_{j,0}|^2\}}\left[\exp\left(-s\sum_{i\in\Phi_p\setminus\{0\}}\zeta\right)\right] \\ &= \mathrm{E}_{\Phi_p}\left[\prod_{i\in\Phi_p\setminus\{0\}} E\left[\exp(-s\zeta)\right]\right] \\ &= \exp\left(-4\pi\lambda_p\int_r^\infty\left(1 - \frac{1}{1+\lambda_s\varsigma K}v^2 dv\right)\right), \end{aligned} \tag{19}$$

where $\zeta = P_t|\mathbf{h}_{j,0}|^2 G(r_{j,0}, \phi_{\text{tilt}}) K d_i^{-(\alpha+1)}$.

And

$$\begin{aligned} L_{I_m}[s] &= \mathrm{E}_{\{\Phi_m\}}\left[\exp\left(-s\sum_{J\in\Phi_f} P_m K l_j^{-(\alpha+1)}\right)\right] \\ &= \mathrm{E}_{\Phi_m}\left[\prod_{i\in\Phi_m\setminus\{c_o\}} E\left[\exp\left(-sP_m K l_j^{-(\alpha+1)}\right)\right]\right] \\ &= \exp\left(-4\pi\lambda_m\int_r^\infty\left(1 - \frac{1}{1+\lambda_s\gamma_u P_m^{-1} r^{\alpha+1}}v^2 dv\right)\right). \end{aligned} \tag{20}$$

Plugging (19) and (20) into (18), (18) can be rewritten as

$$\begin{aligned} F_{\gamma_u}(\gamma_u) = 1 - & \frac{4}{3}\pi\lambda\int_0^\infty \exp\left(-\frac{4}{3}\pi x(\lambda+\xi)\right. \\ & \left. - \gamma_u P_t^{-1} K^{-1}\delta^2 x^{(\alpha+1)/3}\right) dx \int_{r\geq 0} 4\pi r^2 \exp\left(-\frac{4}{3}\right. \\ & \left.\cdot \pi\lambda r^3\right) \exp\left(-\varsigma\delta^2\right) \\ & \cdot \exp\left(-4\pi\left[\lambda_p\int_r^\infty \frac{\lambda_s\gamma_u P_t^{-1} x^2}{\lambda_s\gamma_u P_t^{-1} x^{\alpha+1} + G(v, \phi_{\text{tilt}})} dx\right.\right. \\ & \left.\left. + \lambda_m\int_r^\infty \frac{\lambda_s\gamma_u P_t^{-1} x^2}{\lambda_s\gamma_u P_t^{-1} + x^{\alpha+1}} dx\right]\right). \end{aligned} \tag{21}$$

Finally, the cumulative distribution function of SINR at the legitimate users is obtained by

$$\begin{aligned} F_u(\gamma_u) = 1 - & \int_{r\geq 0} 4\pi r^2 \exp\left(-\frac{4}{3}\pi\lambda r^3\right)\exp\left(-\varsigma\delta^2\right) \\ & \cdot \exp\left(-4\pi\left[\lambda_p\int_r^\infty \frac{\lambda_e\gamma_u P_t^{-1} v^2}{\lambda_e\gamma_u P_t^{-1} + (v/r)^{\alpha+1}} dv\right.\right. \\ & \left.\left. + \lambda_m\int_r^\infty \frac{\lambda_e\gamma_u P_t^{-1} v^2}{\lambda_e\gamma_u P_t^{-1} + (v/r)^{\alpha+1}} dv\right]\right). \end{aligned} \tag{22}$$

Next, the cumulative distribution function of SINR at the eavesdroppers is proposed to analyze

$$\begin{aligned} F_e(\gamma_u) = 1 - & \int_{r\geq 0} 4\pi r^2 \exp\left(-\frac{4}{3}\pi\lambda r^3\right) \\ & \cdot \int_{I_{p,e}\geq 0}\int_{I_{m,e}\geq 0} \exp\left(-\gamma_u P_t^{-1} K^{-1} r^{(\alpha+1)}\left(I_{p,e} + I_{m,e} + \delta^2\right)\right) \\ & \cdot f_{p,e}(I_{p,e}) f_{m,e}(I_{m,e}) dI_{p,e} dI_{m,e} dr. \end{aligned} \tag{23}$$

Similar to the cumulative distribution function of legal users, the cumulative distribution function of eavesdroppers is formulated as follows.

$$\begin{aligned} F_e(\gamma_u) = 1 - & \int_{r\geq 0} 4\pi r^2 \exp\left(-\frac{4}{3}\pi\lambda r^3\right) \\ & \cdot \exp\left(-\gamma_u P_t^{-1} K^{-1} r^{(\alpha+1)}\delta^2\right) \\ & \cdot \exp\left(-4\pi\left[\lambda_p\int_r^\infty \frac{\lambda_e\gamma_u P_t^{-1} x^2}{\lambda_e\gamma_u P_t^{-1} + (x/r)^{\alpha+1}} dx\right.\right. \\ & \left.\left. + \lambda_m\int_r^\infty \frac{\lambda_e\gamma_u P_t^{-1} x^2}{\lambda_e\gamma_u P_t^{-1} + (x/r)^{\alpha+1}} dx\right]\right). \end{aligned} \tag{24}$$

According to the definition of average security rate, the average security rate is expressed as

$$\overline{C} = \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_e}(x)}{1+x}\left(1 - F_{\gamma_u}(x)\right) dx. \tag{25}$$

According to (22) and (23), the average security rate of legitimate users is written by

$$\overline{C} = \frac{\pi\left(\lambda_p + \lambda_m\right)}{\ln 2}\int_0^\infty \psi\, dx. \tag{26}$$

Here,

$$\begin{aligned} \psi &= \frac{\exp\left\{-\pi\lambda_e / \left(\lambda_s\gamma_u P_t^{-1} G^{-1}(x, \phi_{\text{tilt}}) r^{\alpha+1}\right) x^{4/(\alpha+1)}\right\}}{(1+x)\left(\lambda_s\gamma_u P_t^{-1} G^{-1}(x, \phi_{\text{tilt}}) r^{\alpha+1}\right) x^{4/(\alpha+1)} + \pi\left(\lambda_p + \lambda_m\right)}. \end{aligned} \tag{27}$$

From (26), the average security rate is related to the factors such as the density of macrocell BSs and small-cell BSs, the loss coefficient α of large-scale fading, the full-scale multiantenna down tilt ϕ_{tilt}, and the radius distance r. Due to the fact that the parameters such as large-scale fading coefficient and radius distance are determined by the actual scene, as a result, the down tilt ϕ_{tilt} can be adjusted.

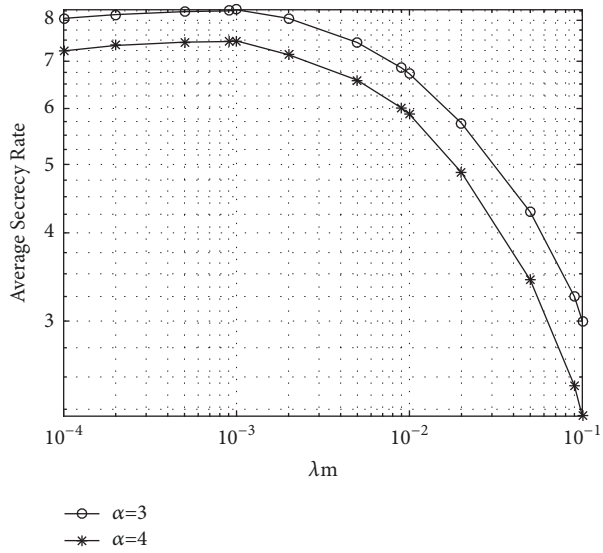

Figure 2: The average security rate versus density of small cells.

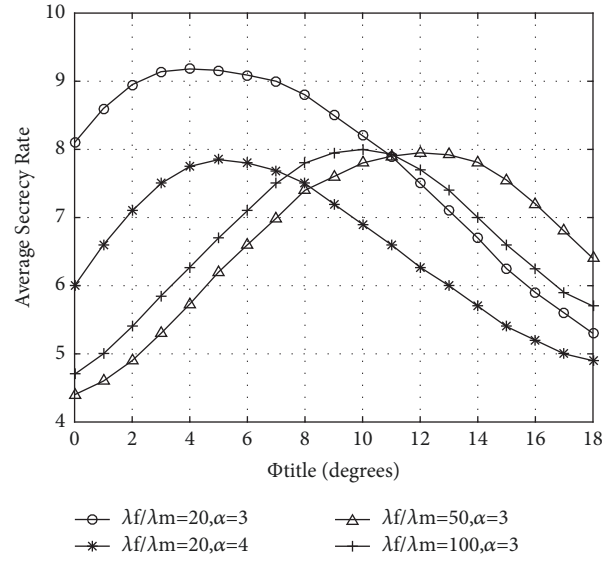

Figure 3: The average security rate versus antenna tilt angle for different density ratios.

4. Simulation Analysis

The macrocell BSs and the small-cell BSs deployed in HetNets are simulated. We assume that the user density is fixed; the coverage radius of the macrocell BSs and the small-cell BSs is set to be 10 km and 50 m, respectively. The transmitting power of the macrocell BSs and the small-cell BSs is ρ = 20 w and ρ' = 100 mw, respectively. The number of row antenna and column antenna equipped with URA is set to be 128 and 64, and the carrier frequency is 3.2 GHz. In these conditions, we propose to analyze the relationship between the average security rate of legitimate users and the distribution density of small-cell BSs in the HetNets and the relationship between the average security rate of legal users and the FD multiantenna down tilt.

As shown in Figure 2, the curve is the average security rate corresponding to the distribution density λ_p (10^{-4}~10^{-1}) of different small-cell BSs. Taking the density λ_m of different macrocell BSs into account, the density of the eavesdropping node is set to λ_e = 0.001 and the threshold of the physical layer security transmission rate is γ_u = 1 bit/s/Hz. It can be seen from Figure 2 that, with the gradual increase in the density of small-cell BSs, the average security rate is gradually reduced, which shows that, with the increase of small-cell BSs, the chance of information leakage increases; therefore, the average security rate of HetNets is reduced.

As shown in Figure 3, the average security rate at the legal users increases first and then decreases, and the users are served by any selected small-cell BSs at different down tilt angles and different BSs density ratios. The BS density ratio denotes the ratio $\eta = \lambda_p/\lambda_m$ of the density of small-cell BSs to the density of macrocell BSs, and the path loss factor is selected as α = 4. It can be seen from Figure 3 that, under different density ratio conditions, the average security rate increases first and then decreases as the down tilt angle changes from small to large. It is not difficult to obtain that the HetNets have the best down tilt angle, so the down tilting can be adjusted to improve the physical layer security. At the same time, the small-cell BSs can also be reasonably arranged to obtain a suitable BSs distribution density ratio; as a result, the optimal average security rate can be obtained.

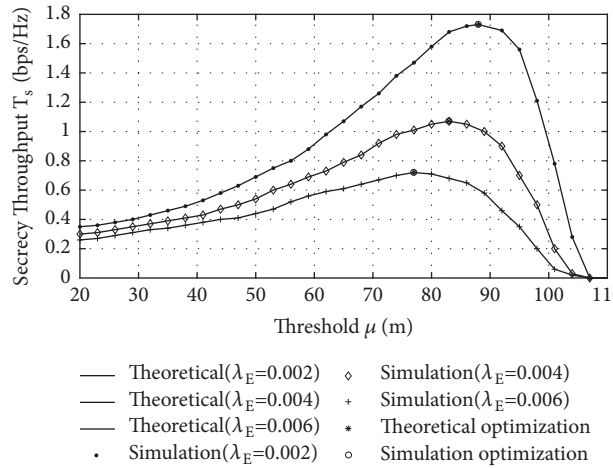

Figure 4: The secrecy throughput versus coverage radius.

Figure 4 represents the performance of the security transmission capacity versus the density of various eavesdropping nodes λ_e. The transmit power of small-cell BSs and the security transmission rate are denoted by ρ' = 100 mw and 4 bit/s/Hz, respectively. It can be seen that the security transmission capacity keeps decreasing as λ_e increases. However, the optimal value of the coverage area is existing in the change of the cell radius.

Figure 5 depicts that as the distribution density of the various eavesdroppers increases, different transmit power of small-cell BSs correspond to different coverage. The larger the transmit power is, the larger the coverage radius is.

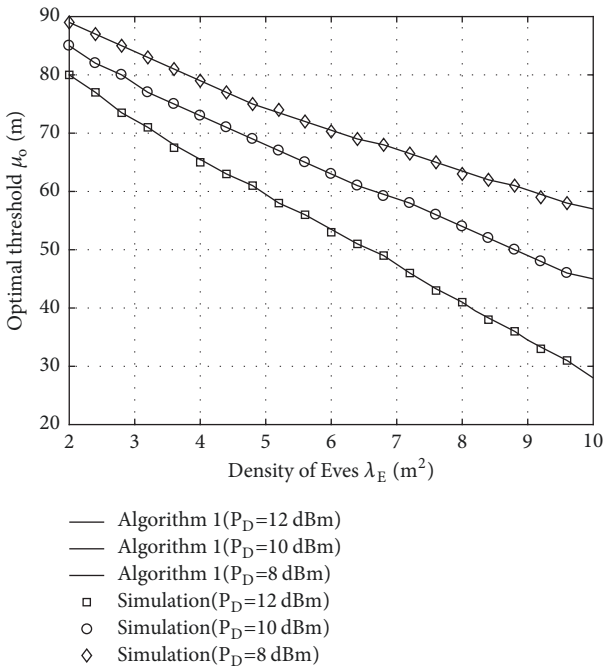

Figure 5: The optimal coverage radius versus density of Eves.

5. Conclusion

In this paper, we research the average security transmission rate of HetNets, and the cumulative distribution function of SINR at the legitimate users and eavesdroppers is deduced. Then the closed expression of average security rate can be obtained, from which we analyze the factors affecting the average security rate. It is possible to improve the average security rate by optimizing the down tilt of the FD antenna. Meanwhile, physical layer security performance can be improved by deploying the small-cell BSs reasonably and optimizing the density ratio of macrocell BSs to small-cell BSs, which provides a theoretical basis for the deployment of HetNets.

Data Availability

The simulation data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the Natural Science Foundation of China (nos. 61501185 and 61302105), the Beijing Natural Science Foundation (no. 4164101), the Hebei Province Natural Science Foundation (no. F2016502062), and the Fundamental Research Funds for the Central Universities (no. 2015MS95).

References

[1] X. Chen, D. W. Ng, W. H. Gerstacker, and H. Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[2] M. Koivisto, M. Costa, A. Hakkarainen, K. Leppänen, and M. Valkama, "Joint 3D positioning and network synchronization in 5G ultra-dense networks using UKF and EKF," in *Proceedings of the 2016 IEEE Globecom Workshops, GC Wkshps 2016*, usa, December 2016.

[3] E. Yaacoub and M. Al-Husseini, "Achieving physical layer security with massive MIMO beamforming," in *Proceedings of the 11th European Conference on Antennas and Propagation, EUCAP 2017*, pp. 1753–1757, March 2017.

[4] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-Layer Security for Proximal Legitimate User and Eavesdropper: A Frequency Diverse Array Beamforming Approach," *IEEE Transactions on Information Forensics and Security*, 2017.

[5] W. Zhao et al., *Beamforming Design for Physical Layer Security and Energy Efficiency Based on Base Station Cooperation*, 2017.

[6] M. Feng and S. Mao, "Interference Management and User Association for Nested Array-based Massive MIMO HetNets," *IEEE Transactions on Vehicular Technology*, 2017.

[7] M. Kamel, W. Hamouda, and A. Youssef, "Performance Analysis of Multiple Association in Ultra-Dense Networks," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3818–3831, 2017.

[8] Y. Wang and Q. Zhu, "Modeling and Analysis of Small Cells Based on Clustered Stochastic Geometry," *IEEE Communications Letters*, vol. 21, no. 3, pp. 576–579, 2017.

[9] S. Vuppala, S. Biswas, and T. Ratnarajah, "Secrecy Outage Analysis of k th Best Link in Random Wireless Networks," *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4478–4491, 2017.

[10] T. Zhang, J. Zhao, L. An, and D. Liu, "Energy efficiency of base station deployment in ultra dense HetNets: a stochastic geometry analysis," *IEEE Wireless Communications Letters*, vol. 5, no. 2, pp. 184–187, 2016.

[11] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1128–1138, 2016.

[12] R. Zhang, X. Cheng, and L. Yang, "Joint power and access control for physical layer security in D2D communications underlaying cellular networks," in *Proceedings of the 2016 IEEE International Conference on Communications, ICC 2016*, pp. 1–6, May 2016.

[13] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, 2011.

[14] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 3, pp. 550–560, 2012.

[15] Z. Pan and Q. Zhu, "Modeling and analysis of coverage in 3-d cellular networks," *IEEE Communications Letters*, vol. 19, no. 5, pp. 831–834, 2015.

[16] A. Omri and M. O. Hasna, "Modelling and performance analysis of 3-D heterogeneous cellular networks," in *Proceedings of the 2016 IEEE International Conference on Communications, ICC 2016*, pp. 1–5, May 2016.

[17] Z. Pan and Q. Zhu, "Energy efficiency optimization in 3-D small cell networks-based sleep strategy," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1131–1134, 2017.