Research on Security of Mobile Communication Information Transmission Based on Heterogeneous Network

Jing Chen, Feng Zhao, and Haiyan Xing
(Corresponding author: Jing Chen)

Department of Information Engineering and Art Design, Shandong Labor Vocational and Technical College
No. 23266, Jingshi Road, Jinan, Shandong 250022, China
(Email: jingc_cj@yeah.net)

(Received Feb. 2, 2019; revised and accepted Dec. 2, 2019)

Abstract

The popularity of the heterogeneous networks has greatly improved the performance of mobile communication technologies, but at the same time, the openness of mobile communication made information security threatened. In order to improve the security of mobile communication, this paper briefly introduced heterogeneous networks and analyzed the physical layer security performance of heterogeneous network through the security rate. Then the Monte Carlo method was used to simulate the average security rate of the two-layer heterogeneous network. The results showed that the increase of the distribution density of the micro-base station in heterogeneous network reduced the average safety rate; the increase of the transmitting power of micro-base station and the signal to interference plus noise ratio (SINR) received by legitimate users increased the average security rate until it was stable; the increase in the distribution density of eavesdropping users in heterogeneous network reduced the average security rate, but when the transmitting power of the micro-base station exceeded 0.4W and the receiving SINR of legitimate users exceeds 30 dB, the average security rate was not affected.

Keywords: Heterogeneous Network; Mobile Communication; Physical Layer Security; Security Rate

1 Introduction

China's upcoming 5G technology will further improve the performance of wireless communication system, and bring more convenience and new related industries [?]. At the same time, high-performance mobile communication technology not only brings convenience, but also brings demanding security performance issues [?]. Compared with traditional wired communication technology, the wireless communication technology has higher openness [?]. If the energy attenuation of wireless signal is not considered, the eavesdropper almost has the same reception condition as legitimate users, that is, eavesdroppers is completely possible to intercept signals containing information in the communication process. The traditional security assurance in mobile communication is accomplished by encrypting the transmitted information, but this method does not fundamentally solve the possibility of information interception. Physical layer security can be achieved between different base stations and users in a heterogeneous network.

The principle of physical layer security of heterogeneous networks is mainly as follows: different wireless communication channels have random characteristics, and random channels generated by different base stations in the network will interfere with other channels to some extent, so the physical layer security of mobile communication can be achieved by rational use of the above characteristics. Relevant studies include: Wang *et al.* [?] comprehensively studied the physical layer security of multi-layer heterogeneous cellular networks with random distribution of base stations, authorized users and eavesdroppers. The simulation results showed that the introduction of appropriate access threshold could significantly improve the security throughput performance of heterogeneous computer network (HCN). Wei *et al.* [?] obtained the signal-to-noise ratio (SNR) of users through the vertical height and downtilt angle of the base station antenna in three-dimensional heterogeneous network. Then, based on the distribution of the base station and users, the expressions of the cumulative SNR distribution function and the average security rate of users were obtained.

The simulation results verified that the expression was correct and the physical layer could be improved by adjusting the downtilt angle. Qi *et al.* [?] studied the user's connection interruption probability, confidentiality interruption and transmission interruption of users in two-tier heterogeneous cellular networks under the confidentiality protection scheme and threshold-based scheme. The simulation results showed that the antenna system, eavesdropper density, predetermined access thresholds and detection area radius all had an impact on the security performance of heterogeneous networks. This paper briefly introduced heterogeneous networks and analyzed the physical layer security performance of heterogeneous network through the security rate. Then the Monte Carlo method was used to simulate the average security rate of the two-layer heterogeneous network.

2 Heterogeneous Network

Heterogeneous network [?] is a mobile wireless network that integrates multiple types of networks with overlapping working areas through intelligent access and provides services for users. The schematic diagram of the model is shown in Figure 1. In real life, whether it is a macro-base station or a micro-base station, its working power is limited. The power of the macro-base station [?] is relatively larger, and the effective working range that can be covered is relatively larger. However, the farther away from the base station, the weaker the signal will be. In addition, different base stations are provided with different services by different operators. If the traditional service mode is adopted, it is very likely that bad signal will occur. The micro-base station in the sub-layer of heterogeneous network can solve this problem. The micro-base station receives the signal from macro-base station and forwards it to users, which is equivalent to expanding and increasing mobile communication information. At the same time, users can still receive the signal directly from the macro-base station in this process, and they can choose to receive the stronger base station signal according to the signal strength of the macro-base station and the micro-base station.

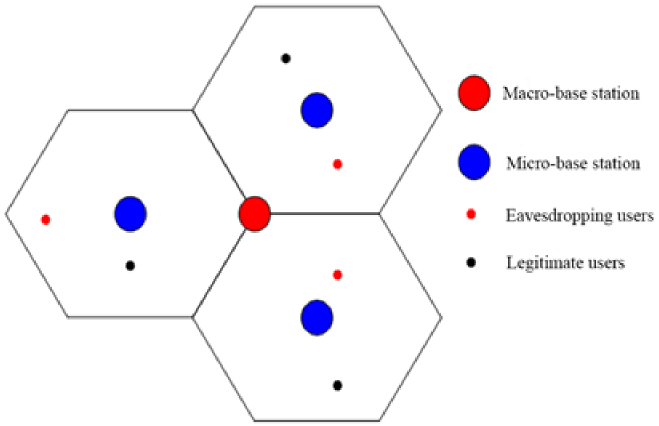

Figure 1: Schematic diagram of heterogeneous network model

According to the heterogeneous network model shown above, the expression of signals that legitimate users and eavesdropping users can receive [?] is:

$$\begin{cases} y_s &= h^H x + n_s \\ y_e &= g^H x + n_e \end{cases} \tag{1}$$

where y_s, y_e respectively stand for legitimate and eavesdropping signals received by user; h, h^H are channel vectors of legitimate users and their corresponding transpose matrices respectively; g, g^H are channel vector of eavesdropping users and their corresponding transposed matrix; x is the message signal of mobile communication; n_s, n_e are noise signals received by the legitimate and eavesdropping users respectively. Gaussian noise that obeys independent distribution is adopted in this model.

3 Physical Layer Security

The physical security model of mobile communication in a heterogeneous network [?] is shown in Figure 2. The base station first transmits a signal, then the legitimate user receives the signal transmitted by the base station through the legitimate channel, and the eavesdropping user receives the signal transmitted by the base station through the eavesdropping channel. The indexes to measure the physical security performance of heterogeneous networks include: signal to interference plus noise ratio (SINR), security rate and security interruption probability [?].

The signal to interference plus noise ratio refers to the ratio of the effective signal power and the interference signal power in the signal received by users in heterogeneous networks, and the higher the ratio is, the higher the signal quality is; at a certain transmission rate, the eavesdropping user in heterogeneous network cannot receive information through eavesdropping channel, while the legitimate user can receive information through the legitimate channel with almost no errors. Then the transmission speed is the security rate, and the maximum security rate is the security capacity of heterogeneous networks. When the security rate of legitimate users receiving information in the network is lower than the set threshold, the channel is judged to be eavesdropped and the communication is interrupted. The probability of the security interruption is the probability of occurrence of the aforementioned event.

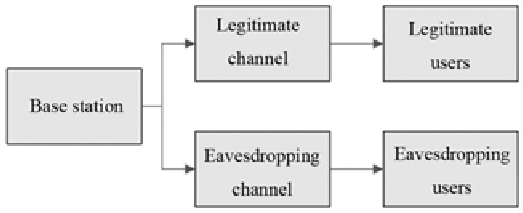

Figure 2: Physical security model of mobile communication

This paper mainly studied the mobile communication security of heterogeneous networks through the security rate. The expression of the security rate of legitimate users in heterogeneous networks [?] is:

$$C = (C_s - C_e)^+ = \max\{C_s - C_e, 0\}, \tag{2}$$

where C_s is the capacity of legal channel between base station and legitimate user; C_e is the capacity of eavesdropping channel between base station and eavesdropping user. The equation for calculating the average safety rate is:

$$\overline{C} \quad = \quad \frac{\int_0^\infty \frac{F_s(x)}{1+x}(1 - F_e(x))dx}{\ln 2} \tag{3}$$

where $F_s(x)$ and $F_e(x)$ are respectively the cumulative distribution function of SINR of legitimate and eavesdrop users. The first step is to get the SINR received by legitimate users and eavesdropping users:

$$\begin{cases} \gamma_s & = \frac{P_t|h_{0,0}|^2 K r^{-(\alpha+1)}}{\sum_{i\in\phi_p\backslash\{0\}} P_t|h_{j,0}|^2 K d_i^{-(\alpha+1)} + \sum_{k\in\phi_m} P_m|g_{j,0}|^2 K l_j^{-(\alpha+1)} + \delta^2} \\ \gamma_e & = \max\left\{\frac{P_t|h_{0,e}|^2 K r_e^{-(\alpha+1)}}{\sum_{i\in\phi_p\backslash\{0\}} P_t|h_{j,e}|^2 K d_i^{-(\alpha+1)} + \sum_{k\in\phi_m} P_m|g_{j,e}|^2 K l_j^{-(\alpha+1)} + \delta^2}\right\} \end{cases} \tag{4}$$

where γ_s and γ_e are SINR received by legitimate users and eavesdropping users under the nearest base station service, respectively; $h_{j,0}$ and $h_{j,e}$ are small-scale fading coefficients between micro-base station and legitimate and eavesdropping users, respectively; $g_{j,0}$ and $g_{j,e}$ are small-scale fading coefficients between macro-base station and legitimate and eavesdropping users, respectively, both of which are Rayleigh Fading [?]; P_t and P_m are the transmission power of micro-base station and macro-base station respectively; K is the signal attenuation factor caused by the path; r is the distance between the user and the base station providing the service; d_i and l_j are the distance from other micro-base stations and macro-base stations to users respectively; α is the path loss index; ϕ_p and ϕ_m respectively represent that the micro-base station and macro-base station obey the Poisson distribution in heterogeneous network; δ^2 is noise power.

In heterogeneous networks, the distribution between micro-base stations and macro-base stations is independent of each other. Within the signal coverage range of the base station, the probability density function of no other base station within the distance between the legitimate user and base station is:

$$f(r) = 4\pi\lambda r^2 \exp(-\frac{4\pi\lambda r^3}{3}), \tag{5}$$

where λ is the distribution density of users; r is the distance between legitimate users and base station. Then, by combining Equation (4) and Laplace transform, the cumulative distribution function of legitimate user's SINR is deduced as follows:

$$\begin{aligned} F_s(x) \quad = \quad & 1 - \int_{r\geq 0} 4\pi r^2 \exp(-\frac{4\pi\lambda r^3}{3}) \\ & \exp(\gamma_s P_t^{-1} K^{-1} r^{\alpha+1} \delta^2) \\ & \exp(-4\pi[\lambda_p \int_r^\infty \frac{\lambda_e \gamma_s P_t^{-1} \chi^2}{\lambda_e \gamma_s P_t^{-1} + (\chi/r)^{\alpha+1}} dx \\ & + \lambda_m \int_r^\infty \frac{\lambda_e \gamma_s P_t^{-1} \chi^2}{\lambda_e \gamma_s P_t^{-1} + (\chi/r)^{\alpha+1}} dx]), \end{aligned} \tag{6}$$

where λ_p and λ_m are the distribution density of micro-base station and macro-base station, respectively. Similarly, the cumulative distribution function of SINR of eavesdropping users can be deduced, which has the same form as legitimate users. The average security rate of legitimate users can be obtained by combining Equation (3) and SINR cumulative distribution function of legitimate users and eavesdropping users:

$$\begin{aligned} \overline{C} \quad = \quad & \frac{\pi(\lambda_p + \lambda_m)}{\ln 2} \\ & \int_0^\infty \frac{\exp(-\pi\lambda_e/(\lambda_s\gamma_s P_t^{-1} r^{\alpha+1}) x^{4/(\alpha+1))}}{(1+x)(\lambda_s\gamma_s P_t^{-1} r^{\alpha+1}) x^{4/(\alpha+1)} + \pi(\lambda_p + \lambda_m)} dx \end{aligned} \tag{7}$$

where λ_s and λ_e are the distribution density of legitimate users and eavesdropping users, respectively.

From the deduced the legitimate user of average security rate, Equation (7), it can be seen that the average security rate of legitimate users is related to multiple factors in the heterogeneous network, including: the transmission power of micro-base stations, the distribution density of micro-base stations and macro-base stations, the distribution density of legitimate and eavesdropping users, the path loss index, the distance between users and base-stations, *etc.*

4 Simulation Experiment

4.1 Simulation Environment

In this paper, the Monte Carlo method [?] was used to conduct simulation analysis on the heterogeneous network. The simulation experiment was carried out in the laboratory server. The server configuration: Windows7 system, I7 processor, 16G memory.

4.2 Simulation Parameters

For the convenience of calculation, the simulation model established in this paper was a two-layer heterogeneous network, and the relevant initial parameters were: the effective working range of macro-base station was 5 km, and the working power was 30 W; the effective working range of the micro-base station was 100 m and the working power was 0.3 W; the antenna array of base station was

125 antennas/row and 60 antennas/column, and the frequency of working radio wave was 800 MHz; the density of legitimate user nodes was 0.01; the density of eavesdropping user nodes was 0.001; the path loss index was 4.0.

4.3 Simulation Project

1) The distribution density of the micro-base station was set between 10-4 and 10-1, and the average security rate of the legitimate users with eavesdropping node density of 0.0005, 0.001, and 0.0015 was simulated separately. Other heterogeneous network parameters were shown as the initial parameters above.

2) The working power of the micro-base station was set between 0.1 W and 0.5 W, and the average security rate of the legitimate users with eavesdropping node density of 0.0005, 0.001, and 0.0015 was simulated separately. Other heterogeneous network parameters were shown as the initial parameters above.

3) The SINR received by legitimate users is set between 20 dB and 35 dB, and the average security rate of the legitimate users with eavesdropping node density of 0.0005, 0.001, and 0.0015 was simulated separately. Other heterogeneous network parameters were shown as the initial parameters above.

4.4 Simulation Results

As shown in Figure 3, in terms of horizontal comparison, the average security rate of legitimate users decreased with the increase of the density of micro-base stations. When the density of micro-base station was between 0.0001 and 0.01, with the increase of the density of the micro-base station, the decrease amplitude of the average security rate was relatively small. When the density of the micro-base station exceeded 0.01, the descending amplitude of the average security rate of legitimate users increased. In terms of longitudinal comparison, under the same distribution density of micro-base stations, the higher the distribution density of eavesdropping users in heterogeneous networks, the lower the average security rate of legitimate users. The above simulation results showed that the increase of distribution density of micro-base stations in heterogeneous networks and the increase of eavesdropping users increased the probability of leakage in the process of information transmission, thereby reducing the average security rate of legitimate users in heterogeneous networks.

As shown in Figure 4, in terms of horizontal comparison, under the same distribution density of eavesdropping users, the average security rate of legitimate users increased with the increase of the power of the micro-base station, and the rising amplitude gradually decreased; when the power of the micro-base station increased to about 0.4 W, the average safety rate reached the maximum and remained stable. In terms of longitudinal comparison, before the power of micro-base station increased to 0.4 W and under the same power, the higher the distribution density of eavesdropping users in heterogeneous networks, the lower the average security rate of legitimate users. But after the power of micro-base station exceeded 0.4 W, regardless of the distribution density of eavesdroppers, the average security rate of legitimate users reached the same fixed value. The above simulation results showed that increasing the transmitting power of micro-base stations in heterogeneous networks could effectively improve the average security rate of legitimate users, and reduce the influence of the density of eavesdropping user distribution on the average security rate after increasing to a certain extent. At the same time, the simulation results also showed that the increase of the power of the micro-base station had a limit to the increase of the average safety rate. Considering the cost, it was not necessary to increase the power of the micro-base station as much as possible.

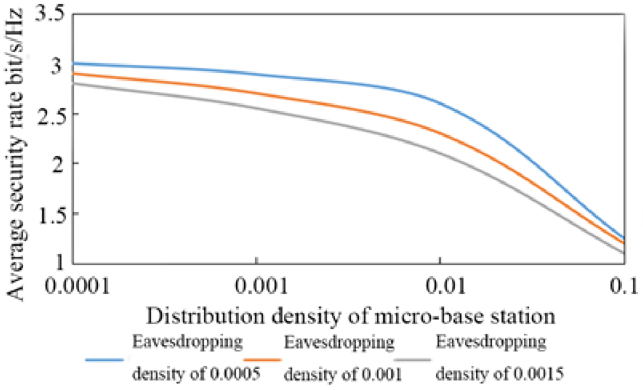

Figure 3: The effect of distribution density of micro-base station on average security rate

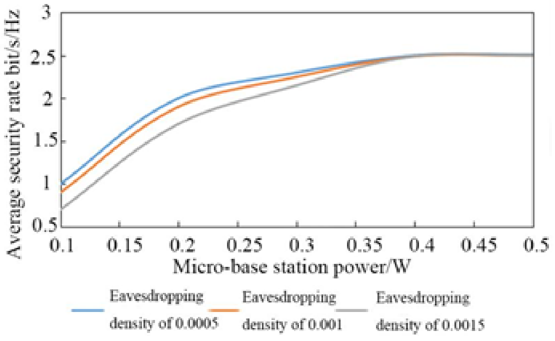

Figure 4: The effect of micro-base station transmitting power on average security rate

As shown in Figure 5, SINR received by legitimate users is adjusted by adjusting the distance between users and the base station and the path loss index α. By horizontal comparison, the average safety rate of SINR between 20 dB and 30 dB increased with the increase of SINR received by legitimate users, and the rising amplitude decreased gradually; after exceeding 30 dB, the average security rate tended to be stable. In the longitudinal comparison, when SINR was between 20 dB and 30 dB, under the same SINR, the higher the distribution density of eavesdropping users, the lower the average security rate of legitimate users. When the SINR received by legitimate users exceeded 30 dB, the average security rate of legitimate users reached the same fixed value regardless of the distribution density of eavesdropping users. The above simulation results showed that improving the SINR of the signal received by the legitimate user could effectively weaken the eavesdropping effect of the eavesdropping users and improve the average security rate.

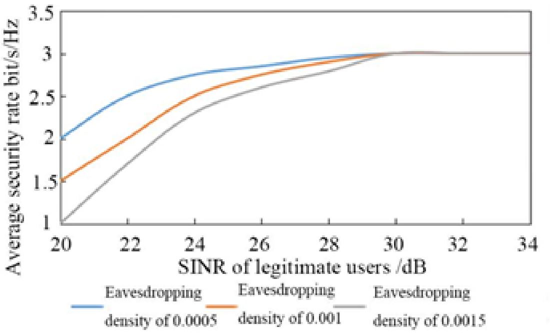

Figure 5: The effect of SINR received by legitimate users on average security rate

5 Conclusion

This paper briefly introduced heterogeneous networks and analyzed the physical layer security performance of heterogeneous network through the security rate. Then the Monte Carlo method was used to simulate the average security rate of the two-layer heterogeneous network. The results are as follows:

1) In heterogeneous network, the increase of the distribution density of micro-base stations reduced the average security rate of legitimate users; the greater the distribution density, the larger the reduction range; at the same time, the increase in the distribution density of eavesdropping users reduced the average security rate;

2) When the micro-base station transmitting power was between 0.1 W and 0.4 W, the increase of transmitting power of micro-base station increased the average safety rate; at the same time, the increase in the distribution density of eavesdropping users reduced the average security rate; after exceeding 0.4 W, the average security rate remained stable and unaffected by the distribution density of eavesdropping users;

3) When SINR received by legitimate users was between 20 dB and 30 dB, the increase of SINR improved the average security rate, and the increase of the distribution density of eavesdropping users reduced the average security rate; after exceeding 30 dB, the average security rate remained stable and was not affected by the distribution density of eavesdropping users.

Acknowledgments

This research was supported by Shandong vocational education teacher studio funding project: Lu teacher's letter [2017] No. 30.

Biography

Jing Chen now works in Shandong Vocational and Technical College of labor. She is a professor. She is interested in computer communication and mobile data transmission technology.

Feng Zhao, born in Jinan, Shandong Province, holds a master's degree. He is now working in Shandong Vocational and Technical College of labor. He is a professor. She is interested in computer network and data communication technology.

Haiyan Xing, born in Dezhou famale, from Jinan, Shandong, China, has gained the master's degree. She is now working in Shandong labor vocational and technical college. She is a lecture. she is interested in big data technology and AI technology.