Research on the Influence of Cooperative Interference on the Physical Layer Security Performance of Wireless Networks in Wireless Communication

Liyun Xing
(Corresponding author: Liyun Xing)

Chongqing Three Gorges Vocational College, Chongqing 404155, China
Email: xingliy1983@outlook.com

(Received Jan. 18, 2023; Revised and Accepted Oct. 21, 2023; First Online Apr. 25, 2024)

Abstract

Information protection is very important in wireless communication. This paper briefly introduces the wireless communication model based on cooperative interference protection and then uses a genetic algorithm (GA) to allocate the node transmission power of cooperative interference. After that, simulation experiments were carried out in MATLAB software to test the performance of a wireless communication network with or without cooperative interference under different numbers of legitimate transmitting nodes. The results showed that the integrity of the information obtained by the eavesdropping nodes in the wireless network was greatly reduced, the probability of secure connection in the network and the system capacity were greatly improved, but the number of nodes participating in cooperative interference was limited. Too many interference nodes can not effectively improve the system capacity and reduce the probability of a secure connection.

Keywords: Cooperative Interference; Genetic Algorithm; Physical Layer; Wireless Communication

1 Introduction

Compared with wired communication technology, wireless communication technology is more free in space deployment because it is not limited by connecting wires and other devices [12]. For users of wireless communication technology, as long as they are within the communication range, they can receive information without space restrictions, which is very convenient. However, compared with wired communication technology, wireless communication technology is more tested in communication security [5]. Wireless communication technology uses electromagnetic waves in a specific frequency band to transmit information, and the broadcast characteristics of electromagnetic waves make the transmitted information directly exposed to the outside world. As long as it is within the range of signal coverage, any device can receive the signal, and there is a possibility of being eavesdropped.

For the problem of wireless communication being eavesdropped, the encryption algorithm is usually used to encrypt the information [9], so as to ensure that the information will not reveal the content even if it is eavesdropped. However, the way of information encryption requires the energy and computing power of communication nodes, and the existing encryption algorithms are challenging to satisfy the demands for both low complexity and high security at the same time. In addition to encrypting information, the physical characteristics of the wireless channel can also be used to ensure communication security. Cooperative interference is a communication security measure that utilizes the physical characteristics of wireless channels. Its basic principle is to optimize the communication quality of legitimate channels or degrade the communication quality of eavesdropping channels.

Zeng *et al.* [15] developed a cross-layer optimization framework for the cooperative interference model in multi-hop networks. Simulation results showed that the session throughput could be significantly improved (more than 50%) by using cooperative interference. Ibrahim *et al.* [3] studied the selection of relay and jammer in two-way cooperative networks to improve their physical layer security. Wang *et al.* [13] put forward a relay and jammer selection strategy to improve the security against eavesdropping attacks. This paper briefly introduces the wireless communication model based on cooperative interference protection and then uses a genetic algorithm (GA) to allocate the node transmission power of cooperative interference. After that, simulation experiments were carried out in MATLAB software.

2 Security Protection of Wireless Network Based on Cooperative Interference

The cooperative interference method is one of the physical protection methods [2]. Its basic principle is that when the sending node sends information to the receiving node, other legitimate nodes in the whole wireless communication area also send interference signals at the same time, and the interference signals are used to reduce the quality of the eavesdropping channel without affecting the legitimate channel as much as possible. Figure 1 shows the wireless communication model based on cooperative interference protection [10]. When sending node S sends information to receiving node D, it also broadcasts the information to the eavesdropping node. At the same time, other legitimate nodes will also send signals to the outside, which are considered interference signals for eavesdropping nodes. The interference signals sent by other legitimate nodes will also interfere with receiving node D. Therefore, when using collaborative interference techniques for wireless communication protection, it is necessary to allocate the transmission power of the sending node in a way that maximizes the interference on eavesdropping nodes and minimizes the interference on receiving nodes [4].

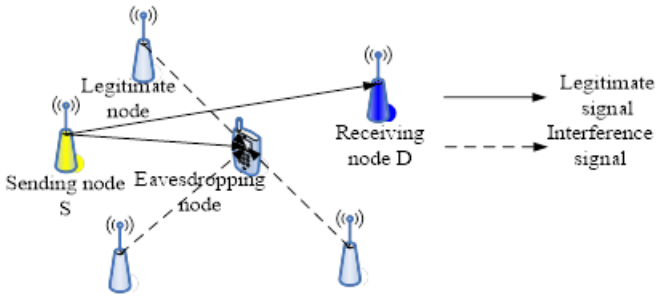

Figure 1: Wireless communication model based on cooperative interference protection

In wireless communication, the received signal-to-noise ratio (SNR) of any receiving node needs to be higher than the minimum demodulation threshold γ_0 to effectively receive information. Therefore, in the cooperative interference protection method, the transmitting node needs to make its transmission power as small as possible to reduce the signal coverage under the premise of ensuring the SNR of the receiving node is higher than γ_0 [6]. Other legitimate nodes used for interference need to increase the transmission power on the premise that the SNR of their receiving nodes is not lower than γ_0, so as to increase the interference to the eavesdropping nodes [1]. In this paper, a GA is used to optimize the transmitting power amplification coefficient to maximize the secure connection probability. The process is as follows.

Step 1. The necessary wireless network-related parameters are input, including γ_0, U (the set of transmitting nodes), D (the set of receiving nodes), D^*_{mat} (the adjacency matrix of the distance between transmitting nodes and receiving nodes), and H^*_{mat} (the channel gain matrix).

Step 2. The chromosome population required by the GA is generated. The gene segment in the chromosome represents the transmitting power amplification coefficient of a legal node, and a chromosome represents a group of power amplification coefficients, which also represents a transmission power allocation scheme. When the chromosome population is randomly generated, the power amplification coefficient of a legitimate node represented by a gene segment must be an integer multiple of 0.5 and no less than 1, and it can not exceed the preset maximum value. The length of the chromosome depends on the number of legitimate transmitting nodes used for interference.

Step 3. The fitness value of each chromosome in the population is computed. The ultimate goal is to maximize the safe connection probability, so it is taken as the fitness value of the chromosome. The formulas are:

$$\begin{cases} SCP_{d^*} = \\ \quad 1 - exp[\frac{-D^{\alpha}_{u^*e} N_0 |h_{u^*d^*}|^2}{D^{\alpha}_{u^*d^*}(N_0 + \sum_{i=1}^{N} P_{u_i} |h_{u_i d^*}|^2 D^{-\alpha}_{u_i d^*})}] \\ \quad \times \prod_{u_i} [\frac{P_{u_i} |h_{u^*d^*}|^2 D^{\alpha}_{u^*e}}{D^{\alpha}_{u^*d^*} D^{\alpha}_{u^*e} (N_0 + \sum_{i=1}^{N} P_{u_i} |h_{u_i d^*}|^2 D^{-\alpha}_{u_i d^*})}] \\ P_{u^*} \simeq \frac{\gamma_0 D^{\alpha}_{u^*d^*} N_0}{|h_{u^*d^*}|^2} \\ P_{u_i} = A_i \frac{\gamma_0 D^{\alpha}_{u_i d_i} N_0}{|h_{u_i d_i}|^2} \end{cases} \quad (1)$$

where SCP_{d^*} is the secure connection probability of sending node u^* and receiving node d^* [14], α is the path loss coefficient [7], D_{u^*e} is the transmission distance between u^* and eavesdropping node e, N_0 is Gaussian white noise, $|h_{u^*d^*}|^2$ is the channel gain between u^* and d^*, $D_{u^*d^*}$ is the transmission distance between u^* and d^*, N denotes the number of legitimate transmitting nodes used for interference, u_i is the i-th legitimate transmitting node used for interference, d_i is the corresponding receiving node of u_i, P_{u_i} is the transmitting power of u_i, $|h_{u_i d^*}|^2$ is the channel gain between u_i and d^*, $D_{u_i d^*}$ is the transmission distance between u_i and d^*, $|h_{u_i d_i}|^2$ is the channel gain between u_i and d_i [8], $D_{u_i d_i}$ is the transmission distance between u_i and d_i, and A_i is the transmitting power amplification coefficient of u_i.

Step 4. Whether the GA terminates the optimization is determined. The termination conditions include: the number of iterations reaches the preset number or the population fitness converges to stability. If the termination condition is reached, the next step is entered. If not, the genetic operation is performed. Crossover

means exchanging the homogenic fragments of the two chromosomes based on the crossover probability, and mutation means randomly changing the gene fragments in the chromosome based on the mutation probability. In this paper, the random change in accordance with the restrictions is performed on A_i. After the genetic operation, return to Step 3.

Step 5. After the termination of the GA, the transmitting power of each transmitting node that can maximize SCP_{d^*} is obtained. Whether there is d_i whose SNR is smaller than γ_0 under this transmitting power is judged. If not, the transmitting power allocation result of each transmitting node is output. If it exists, the sending node with the smallest $|h_{u_i d_i}|^2 D_{u_i d_i}^{-\alpha}$ in the set of legitimate sending nodes used for interference is deleted, the corresponding receiving node is also deleted, and it returns to Step 2.

3 Simulation Experiment

3.1 Experimental Setup

Simulation experiments were carried out in MATLAB software [11]. The wireless network parameters used for the simulation experiments are shown in Table 1, in which the number of legitimate sending nodes including specific sending nodes was set to 3, 4, 5, 6, 7, 8, and 9 respectively, and the corresponding number of receiving nodes was also the same. The simulation experiments were designed to test the impact of the number of interfering nodes on the protection of wireless communication.

The GA was used to adjust the transmitting power, and the related parameters are as follows. The population size was 15; the first three chromosomes were duplicated as the offspring. The crossover probability was 0.5, the mutation probability was 0.1, and the iteration number was 100.

According to the above conditions, 5,000 random experiments were carried out on the wireless network for each number of legitimate sending nodes. In each experiment, a specific sending node sent 1 MB of data to the corresponding receiving node, and the eavesdropping node tried to receive it. To improve testing efficiency, data transmission in the simulation experiment was not encrypted.

3.2 Test Results

In the random experiments with different numbers of legal sending nodes, a specific sending node sent 1 MB of data to the corresponding receiver node, and in each random experiment, the eavesdropping node eavesdropped on the sent information. The average integrity of the data obtained by the eavesdropping node with or without cooperative interference is shown in Figure 2. It can be seen that in the case of no cooperative interference, the average integrity of the information obtained by the eavesdropping node was maintained at about 90% with the increase in the number of legitimate transmitting nodes because the transmitted information was not encrypted in the experiment. The reason why it failed to reach 100% is that the eavesdropping node was far away from the transmitting node in the random experiment, which reduced the SNR of the eavesdropping node and failed to obtain the transmitted data. In the case of cooperative interference, the average integrity of the information that can be obtained by the eavesdropping node was greatly reduced, and it continued to decrease with the increase in the number of legitimate sending nodes.

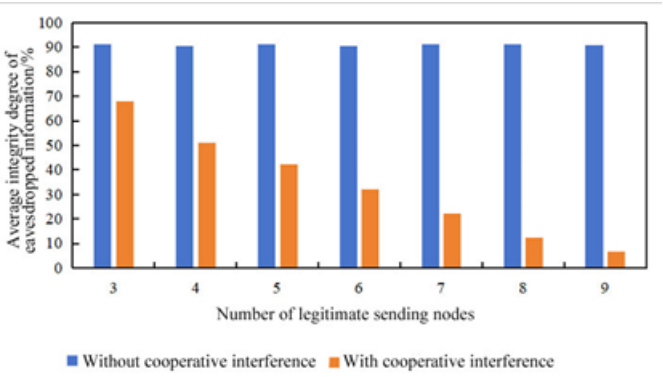

Figure 2: Information integrity of eavesdropping nodes with or without cooperative interference under different numbers of legitimate sending nodes

In the random experiments with different numbers of legitimate sending nodes, the secure connection probability with or without cooperative interference is shown in Figure 3. It can be seen that in the case of no cooperative interference, the secure connection probability in the simulated wireless network did not change significantly and basically stayed at about 71%. In the case of cooperative interference, the secure connection probability in the simulated wireless network first increased and then decreasesd with the increase in the number of legitimate sending nodes. When the number was 6, the secure connection probability was the largest. The reason is that in the case of no cooperative interference, the information of the sending node might be obtained by the eavesdropping node. However, with cooperative interference, the channel of the eavesdropping node was interfered by other nodes, which reduced the probability of being eavesdropped and improved the probability of secure connection. With the increase in the number of legitimate sending nodes, the interference to the eavesdropping node increased, and the probability of a secure connection was also improved. However, when the number of legitimate transmitting nodes was too large, the interference signals generated by them also interfered with the normal receiving nodes.

In the random experiments with different numbers of legitimate transmitter nodes, the system capacity with or

Table 1: Wireless network simulation parameters

Parameter	Setting
Area specification	300 m × 300 m
Number of legitimate sending nodes	4, 5, 6, 7, 8, 9 {3}
The transmission distance of the corresponding sending and receiving nodes	5 m ∼ 15 m
The transmission distance between the sending node and other receiving nodes	20 m ∼ 120 m
The transmission distance between the eavesdropping node and the specific sending node	10 m ∼ 50 m
Channel gain between nodes	Randomly generated, with a mean of 1
α	3
N_0	1
A_i	Its value ranges from 1 to 6 and is a multiple of 0.5
γ_0	5 dB

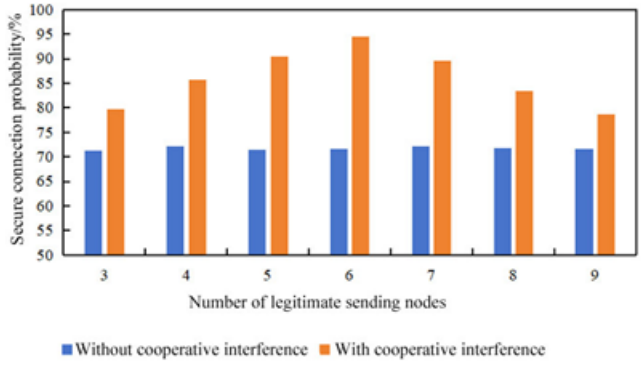

Figure 3: Secure connection probability under different numbers of legitimate sending nodes with or without cooperative interference

without cooperative jamming is shown in Figure 4. The system capacity refers to the transmission rate of wireless communication in a unit frequency band. It can be seen that with the increase in the number of legitimate transmitting nodes, the system capacity in the wireless network without cooperative interference almost did not change. However, the system capacity in the wireless network with cooperative interference first increased and then tended to be stable. The reason is that in the case of no cooperative interference, because eavesdropping nodes stole and interfered with the transmitted information, the system capacity failed to increase after the addition of legitimate transmitting nodes. When there was a cooperative interference, the eavesdropping node was affected, and the probability of a secure connection between the sending node and the receiving node increased, leading to an increased amount of information that could be transmitted, so the system capacity increased. However, when the number of legitimate transmitting nodes was too large, the interference signal affected the receiving node, causing the interference node to fail in correctly demodulating information.

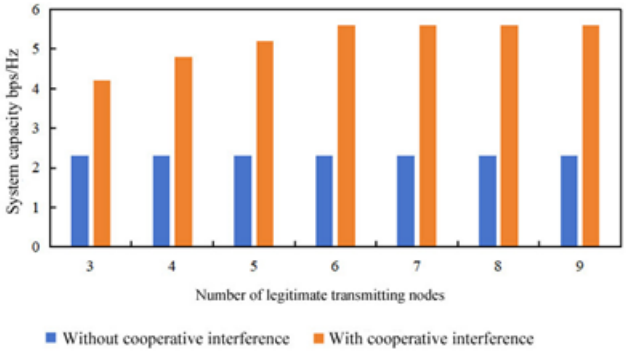

Figure 4: System capacity with and without cooperative interference for different numbers of legitimate transmitting nodes

4 Conclusion

This paper used a GA to allocate the node transmitting power under cooperative interference and then carried out simulation experiments in MATLAB software. In the experiment, the performance of a wireless communication network with or without cooperative interfer-

ence under different numbers of legitimate transmitting nodes was tested. With the increase in the number of legitimate sending nodes, the integrity of information obtained by the eavesdropping nodes in the network without cooperative interference was almost unchanged, and the integrity of information in the network with cooperative interference was not only smaller but also decreased gradually. With the increase in the number of legitimate sending nodes, the secure connection probability of the network without cooperative interference was almost unchanged, while the secure connection probability of the network with cooperative interference first increased and then decreased. It was the highest when the number of sending nodes was 6. With the increase in the number of legitimate sending nodes, the system capacity of the network without cooperative interference remained unchanged, and the system capacity of the network with cooperative interference gradually increased and tended to be flat after the number reached 6.

References

[1] X. Hu, C. Kai, Z. Guo, J. Gao, "A fast forward full-duplex cooperative relay scheme for securing wireless communications," *IEEE Signal Processing Letters*, vol. 26, no. 5, pp. 775-779, 2019.

[2] K. Z. Huang, Y. Hong, W. Y. Luo, S. B. Lin, "A method for physical layer security cooperation based on evolutionary game," *Journal of Electronics & Information Technology*, vol. 37, no. 1, pp. 193-199, 2015.

[3] D. H. Ibrahim, E. S. Hassan, S. A. El-Dolil, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *Computers & Security*, vol. 50, no. may, pp. 47-59, 2015.

[4] N. Kolokotronis, M. Athanasakos, "Improving physical layer security in DF relay networks via two-stage cooperative jamming," in *Signal Processing Conference*, pp. 1173-1177, 2016.

[5] B. Li, J. Zhou, Y. Zou, F. Wang, W. Cao, "Security and reliability trade-off analysis of joint user and jammer selection in the face of co-channel interference," *IET Communications*, vol. 13, no. 6, pp. 2601-2608, 2019.

[6] C. Li, Y. Liu, Q. Xu, Y. Tang, "Self-interference cancellation with frequency offset and nonlinear distortion suppression for cooperative jamming communications," *IEEE Communications Letters*, vol. 23, no. 11, pp. 2091-2094, 2019.

[7] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46-49, 2017.

[8] H. Long, W. Xiang, Y. Li, "Precoding and cooperative jamming in multi- antenna two-way relaying wiretap systems without eavesdropper's channel state information," *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 6, pp. 1309-1318, 2017.

[9] Q. Ning, T. Yang, B. Chen, X. Zhou, C. Zhao, X. Yang, "Cooperative transmission of wireless information and energy in anti-eavesdropping UAV relay network," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1283-1292, 2021.

[10] A. E. Shafie, D. Niyato, N. Al-Dhahir, "Security of rechargeable energy-harvesting transmitters in wireless networks," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 384-387, 2016.

[11] H. A. Shah, I. Koo, "Improving physical layer security via cooperative diversity in energy-constrained cognitive radio networks with multiple eavesdroppers," *International Journal of Communication Systems*, vol. 32, no. 14, pp. e4008.1-e4008.18, 2019.

[12] S. Vahidian, S. Aissa, S. Hatamnia, "Relay selection for security-constrained cooperative communication in the presence of eavesdropper's overhearing and interference," *IEEE Wireless Communications Letters*, vol. 4, no. 6, pp. 577-580, 2015.

[13] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, Y. Sun, "Strategic antieavesdropping game for physical layer security in wireless cooperative networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 9448-9457, 2017.

[14] W. Yang, L. Xiao, L. Sun, Q. Li, "Cooperative transmission against impersonation attack using inter-session interference in two-hop wireless networks," in *IEEE Trustcom/BigDataSE/ISPA*, pp. 104-110, 2015.

[15] H. Zeng, X. Qin, X. Yuan, Y. Shi, Y. T. Hou, W. Lou, "Cooperative interference neutralization in multi-hop wireless networks," *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 889-903, 2018.

Biography

Liyun Xing, born in September 1983, has obtained a master's degree. She is working at Chongqing Three Gorges Vocational College. She is interested in computer application technology and vocational education.