

Research on Collaborative Communication Strategy Based on Physical Layer Security

Wei Ding, Yu Zhang, and Yu Liu

Xidian University, Xi'an, China

Abstract. Collaborative communication and physical layer information security are two valuable aspects in the field of modern wireless communication. Combining the characteristics of the two, the physical layer security model based on cooperative communication is studied, and the amplification and forwarding strategy and cooperation among them in this paper, the best security capacity of congestion strategy is analyzed. In the light of the fact that related researches do not involve the analysis of performance scenarios, the comparison of security capacity performance under different scenarios is carried out for amplification forwarding strategy and collaborative congestion strategy. Simulation studies show that the amplification and forwarding strategy is more stable and less susceptible to scenario changes than the cooperative congestion strategy. In addition, the performance improvement caused by the increased number of relay antennas is also equivalent to increasing the number of trunks.

1. Foreword

With the rapid development of wireless communication technology, people have higher and higher requirements on the data transmission rate, service quality and transmission security of the communication system. In general, security refers to the degree of harm to the system caused by external factors such as eavesdropping or attacks or abnormal accidents during the transmission. Due to limited spectrum resources and the decline of the wireless environment and the openness of the media, the security of wireless communications is increasingly challenged. How to ensure the security of signal transmission more effectively during the communications have become today's Research hot issues.

At present, the information security technology used in wireless communication system is mainly transplanted in the wired communication system, and the more is the research of system security from the network layer and above layers. However, the physical layer security technology has not attracted sufficient attention of researchers. However, with the rapid development of physical layer transmission technologies such as channel coding technology, multi-antenna technology and spread spectrum technology, the physical layer security technology is facing more opportunities and challenges.

2. Channel model

2.1. Three-node eavesdropping channel model

The first to study physical layer security was Wyner, who introduced the concept of wire-tap channel in 1975 and introduced a three-node eavesdropping channel model: a three-node eavesdropping channel model that includes a source S for one purpose Node D and an eavesdropper E, the source S sends a message to the destination node D. Because of the broadcast nature of the wireless propagation



environment, the eavesdropper E in the transmission process can also receive signals from the source S and analyze them. In this model, the channel between the source node S and the destination node D is the primary channel, and the channel between the source node S and the eavesdropper E is the eavesdropping channel. Wyner describes this model from the perspective of information security, and points out that when the primary channel condition is better than the eavesdropping channel condition, it can find a theoretically secure way to achieve a positive secure capacity without coding only by means of coding. So that eavesdroppers can hardly obtain any information and thus realize the secure transmission of information through the physical layer. Wyner eavesdropping channel model for the physical layer of information security provides a guiding idea, but also the basis for the next study.

2.2. Cooperative Communication Eavesdropping Channel Model

Based on the three-node eavesdropping channel model, the source S not only sends the information directly to the destination node D but also sends the corresponding information to the destination node D through multiple relay nodes R, effectively overcoming Path fading effect, improve system performance. Similar to the three-node eavesdropping channel model, the eavesdropper E can also obtain the information sent by the source S to the destination node D through the links from the source S to the E and the links from the relay R to the E, causing the information to be leaked and the information reduced Security. Cooperative communication eavesdropping channel model is shown in Figure 1 below.

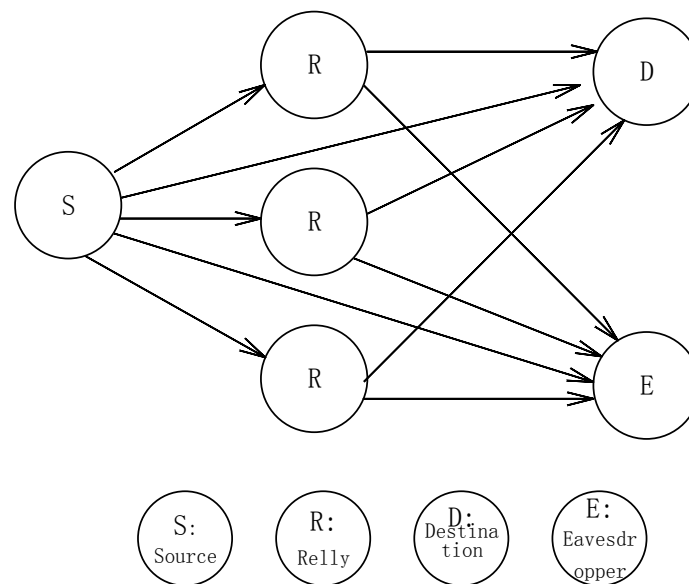


Figure 1. Cooperative communication eavesdropping channel model

2.3. Safety capacity

Security capacity is a key parameter for studying the security technology of wireless network physical layer and is the next major research object. Security capacity is defined as the maximum achievable communication rate at which confidential information is reliably received by the intended receiver and the illegal receiver cannot obtain any useful information. In the additive Gaussian channel, it is equivalent to the difference between the channel capacity of the main channel and the eavesdropping channel. According to the Shannon theorem in information theory, in the eavesdropping channel model, the definition of the channel capacity RD and RE that can be obtained by the main channel and the eavesdropping channel are as follows:

$$RD = \lg 2(1 + SNRD) \quad (1)$$

$$RE = \lg 2(1 + SNRE) \quad (2)$$

Where SNRD and SNRE are the instantaneous signal-to-noise ratios at the main channel and at the eavesdropping channel, respectively.

Therefore, the safety capacity RS can be expressed as:

$$RS = RD - RE = \lg 2(1 + SNRD) - \lg 2(1 + SNRE) \quad (3)$$

From the definition of security capacity, we can see that if the instantaneous signal-to-noise ratio of the eavesdropping channel is greater than the signal-to-noise ratio of the primary channel, the security capacity will have a negative value and the information security cannot be guaranteed. For the study of physical layer security, increasing the value of the security capacity is crucial.

3. two kinds of relay cooperation strategy

Consider a co-channel eavesdropping channel model similar to the one in Figure 1, which includes a transmit source point S, M relay Rs (R1... RM, respectively), a destination node D and an eavesdropper E. The source S, the destination node D and the eavesdropper E are configured with a single antenna, and the relay R can be configured with a single antenna or multiple antennas. The channel states for all channels are assumed to be known.

3.1. Relay amplification forwarding

In the relay amplification and forwarding (AF) strategy, the relay node receives the information of the source S, and then amplifies and forwards directly. AF strategy consists of two stages. In the first phase, the source S broadcasts the encoded symbol x to M trunks, and the signals y_r [$y_{r1} \dots y_{rM}$] received by the relay are as follows:

$$y = \sqrt{P_S} h_{SR} * x + n_r \quad (4)$$

In equation (1), P_S is the transmit power of source S, $h_{SR} \triangleq [h_{sr1} \dots h_{srM}]$ is the channel gain matrix between source S and M relays R, $n_r \triangleq [n_{r1} \dots n_{rM}]$ is the Gaussian white noise received by each relay.

In the second phase, the M relays forward the received signal y_r , including the wanted signal and the noise signal, while each relay also adds a weight factor $w \triangleq [w_1, \dots, w_M]^T$. Therefore, the actual signal relayed to $w y_r$.

3.2. Relay collaboration congestion

In relay cooperative congestion (CJ) strategy, when the source S transmits the signal x to the destination node D, the relay R simultaneously transmits an interference signal z with a weight factor independent of the transmission signal x to confuse the eavesdropper E to receive to the signal. The destination node D receives the signal as

$$y_d = \sqrt{P_S} h_{RD} * \text{diag}\{w|h_{SR} * x + h_{RD} * \text{diag}\{w\}n_r + n_d \quad (5)$$

Eavesdropper E receives the signal as

$$y_e = \sqrt{P_S} h_{RE} * \text{diag}\{w|h_{SR} * x + h_{RE} * \text{diag}\{w\}n_r + n_e \quad (6)$$

HSD is the channel gain coefficient between source S and destination D, h_{SE} is the channel gain function between source S and eavesdropper E, and other parameters are the same as those in AF strategy.

4. safety capacity performance simulation analysis

For the physical layer of security research, the most important research object is the security capacity. In the following, the security capacity performance simulation of different scenarios will be mainly focused on the security model of cooperative communication eavesdropping based on AF strategy and CJ strategy. Including the performance analysis of the security capacity when the trunks, eavesdroppers and the destination nodes are in different positions respectively; the influence of the number of relays on the security capacity; the influence of the number of relay antennas on the security capacity; the influence of the relay power on the security capacity; AF strategy and CJ strategy comparison and so on. The simulation platform used is MATLAB.

The basic simulation scenario is as follows: the source point S is located at (0, 0) of the coordinate axis, the relay R is randomly distributed in a circle with a radius of 0.1, the position of the circle is variable, the positions of the destination node D and the eavesdropper E are also variable. The 1 on the axis is equivalent to 500 m of the actual distance. The transmission power P_S of source S is 10 W, the total power of relay is 10 W, and the σ^2 of white Gaussian noise is 10^{-5} W.

4.1. Destination node location

In order to study the influence of the change of destination node on security capacity, based on the above basic simulation scenario, fixed eavesdropper E is located at (2, 0), fixed relay circle is at position (1, 0), and relay the number of eavesdroppers D is variable, and all the trunks are configured with a single antenna. The total power of the relay is 10 W. The cooperative relay strategies adopted include the AF strategy and the CJ strategy.

The result of the simulation is shown in Figure 2. When the destination node moves from (1.2, 0) to (3.2, 0), that is, from the source point S to the source point far away from the source point, the security capacity is decreasing both in the AF strategy and in the CJ strategy. CJ strategy security capacity decline trend faster, AF strategy is relatively more gentle. It can be seen that the AF strategy is less affected by the location of the destination node, and the CJ strategy is more affected by the location of the destination node. Therefore, in contrast, the AF strategy is superior to the CJ strategy in this respect.

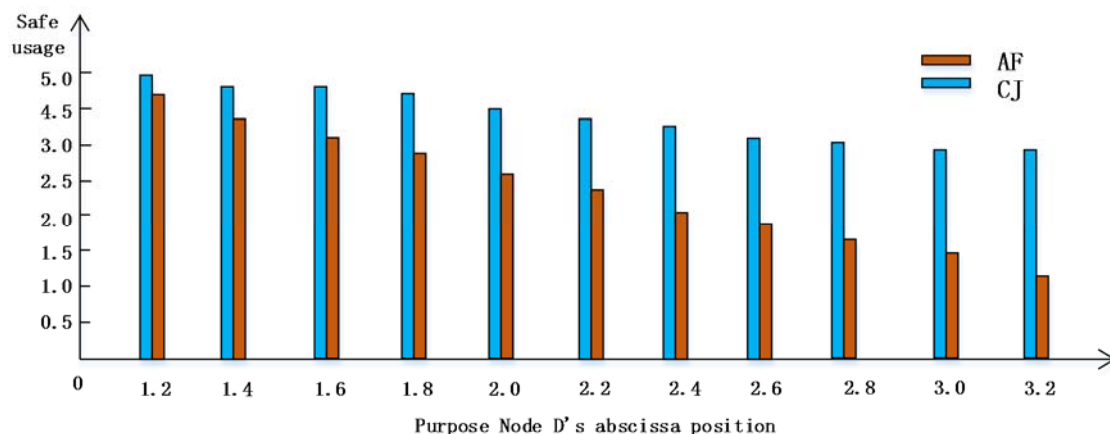


Figure 2. The change of safety capacity during the process of moving the node D from (1.2, 0) to (3.2, 0)

4.2. Eavesdropping position

In order to study the impact of eavesdropping location changes on security capacity, based on the basic simulation scenario, the location of the fixed destination node D is (2, 0), the position of the fixed relay circle is (1, 0), the number of relays 5, eavesdropper E position is variable, all the trunks are configured with a single antenna, using the cooperative relay strategy includes AF strategy and CJ strategy.

The result of the simulation is shown in Figure 3. When eavesdropper E moves from (1.2, 0) to (3.2, 0), that is, from near source point S to far from the source point, the change in security capacity is very

small, indicating wherever the eavesdropper is located, Through the AF and CJ two strategies can get a stable safety capacity. However, the security capacity obtained by the AF strategy is significantly greater than the CJ strategy, which is probably 50% larger than the CJ strategy. Therefore, both AF and CJ strategies are reliable and stable cooperative communication physical layer security policies in this respect. However, AF strategies have larger security capacity and better performance.

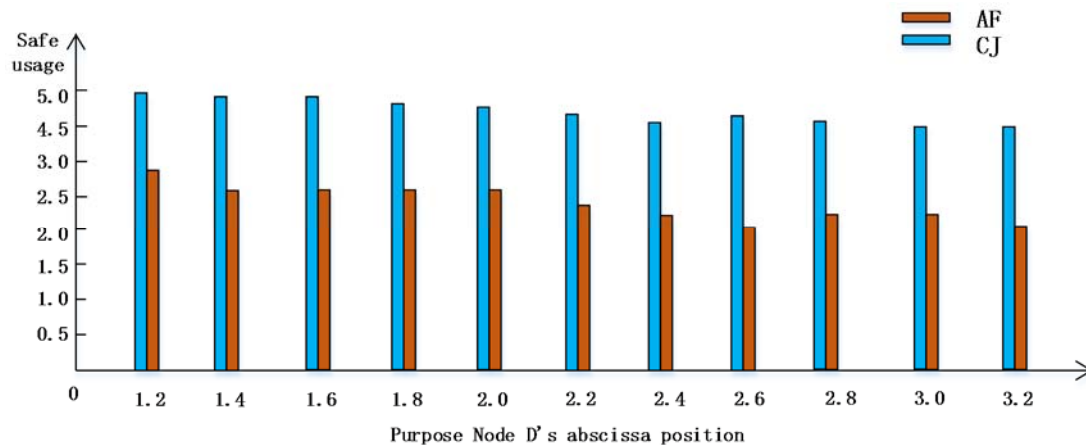


Figure 3. Eavesdropper E moves from (1.2, 0) to (3.2, 0), the change of safety capacity

4.3. Relay position

In order to study the influence of the change of relay position on the safety capacity, based on the simulation scenario above, the location of the fixed destination node D is (2, 0), the position of the fixed eavesdropper E is (2.5, 0), the relay R The location of the circle is variable, the number of relays is 5, and all the trunks are configured with a single antenna. The adopted cooperative relay strategy is an AF strategy.

The result of the simulation is shown in Figure 4. When the relay R moves from (0, 0) to (0.6, 0), the safety capacity increases and the safety capacity at (0.6, 0) is maximized. When the relay R moves from (0.6, 0) to (2, 0, 0), That is, farther and farther from the source point S, and closer to the destination node D and eavesdropper E, the total security capacity tends to decrease. From the simulation results, it can be seen that in the tapping model under AF strategy, there is an optimal relay position point.

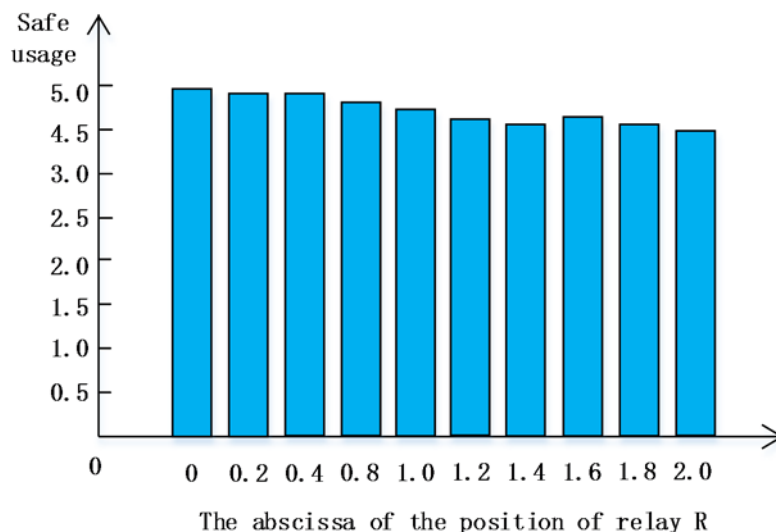


Figure 4. Relay R position from (0, 0) to (2, 0) during the change of safety capacity

4.4. AF strategy comparison CJ strategy

From the above simulation results of multiple scenarios, AF strategy is superior to CJ strategy in terms of secure capacity performance. From a theoretical perspective, in the eavesdropping channel model, the AF strategy improves the signal-to-noise ratio of the eavesdropping node while enhancing the signal-to-noise ratio of the eavesdropping node. However, by adjusting the relaying weight, Noise ratio while greatly reducing the signal to noise ratio of the eavesdropping node; CJ strategy reduces the signal to noise ratio of the target node while reducing the signal to noise ratio of the eavesdropping node, and adjusting the relay weight can reduce the amplitude of the signal to noise ratio drop of the destination node. For both strategies, the tapping capacity tends to be 0 by adjusting the weight of the relay. Therefore, the main factor affecting the safety capacity is the capacity of the primary channel, that is, the signal-to-noise ratio at the destination node. Therefore, the AF strategy that enhances the signal-to-noise ratio of the destination node is superior to the CJ strategy that reduces the signal-to-noise ratio of the destination node in the capacity performance of security.

5. Conclusion

The physical layer security mechanism under collaborative communication is studied, the optimal security capacity of the AF and CJ policies is analyzed, and the AF and CJ policies are compared in a number of different scenarios Detailed performance comparison and theoretical analysis. Simulation results show that the AF strategy outperforms the CJ strategy in terms of safety capacity. In addition to the larger safety capacity, the change of safety capacity is more stable and less affected by the change of the location of the destination node. In addition, the effect of the number of relays and the number of antennas on the security capacity performance is also compared. The simulation results show that the performance gain of adding one antenna and adding one relay is very close, that is, the method of adding an antenna can replace the method of adding the relay Way to carry out collaborative communication.

References

- [1] Zhang Junyi; Yang Yixian; Physical Layer Analysis of Wireless RF Injection [J]; Radio Engineering; 2009-02.
- [2] Chen Yongjian; Basic Concepts of Communication Physical Layer (1) [J]; Information Systems Engineering; 1998-01.
- [3] LI Jin-hui, SUN Xiao-juan, ZHANG Ming-de, DING Dong; Research on Physical Layer Data Flow in Multimedia Optical Fiber Industrial Private Network [J]; Journal of Applied Sciences; 2002-04.
- [4] Zhang Rui; Li Bo; Research on Precise Modeling and Simulation of Wireless Network Physical Layer [J]; Microcomputer Applications; 2010-06.
- [5] Liu Feng; Information Security of Wireless Physical Layer [J]; Computer CD Software and Applications; 2012-03.