Performance Analysis of Physical Layer Security under the Cooperation of Multiple Malicious Jammer Relays

Shengbin Lin, Qingfeng Liu, Kaizhi Huang, and Wen Wang

***Abstract*—**This paper considers a communication network that includes a transmitter, a legitimate receiver, an eavesdropper and a number of malicious jammer relays which help the eavesdropper. The multiple malicious jammer relays cooperate sending linear amplification of the eavesdropping signals and noise to reduce secrecy rate. Firstly, we build a complex Gaussian model and the malicious jammer relays eavesdrop the signal from the transmitter. Then, they send appropriate linear amplification of the eavesdropping signals and noise in the limited total power according to their channel states. Besides, we deduce secrecy rate on Gaussian noise and structured noise scenarios and conclude that the secrecy rate under Gaussian noise is bigger than that under structured noise. Finally, numerical simulation results show the average secrecy rate of cooperation relay is 0.15bits/s/Hz less than that of one relay under Gaussian noise and 0.05bits/s/Hz less than that of one relay under structured noise.

Keywords*—secrecy rate, malicious jammer relay, cooperative jamming*

I. Introduction

WIRELESS networks have the characteristics of broadcast, which brings convenience for illegal users to wiretap, interfere, or even attack the network. Therefore, a series of security problems are raised. In response to these threats, traditional solutions are encrypting the information at the high level. But there is great challenge to distribute and manage keys for the dynamic changes in the network topology. At the same time, the demand of frequently updating user key increases the complexity of the existing encryption algorithm. Recently, physical layer security, considering the nature and the characteristics of the wireless channel, makes use of coding, modulation and other communication technologies to ensure legitimate communication. By increasing the difficulty for the eavesdropper to intercept and restore the signal, secure transmission of the wireless network can be achieved [1]-[3].

For an eavesdropping scene with one transmitter, one legitimate receiver and one eavesdropper, the physical layer security methods are mainly divided into three categories: signal processing technologies based on the characteristics of the wireless channel, such as artificial noise [4], consistency key generation technologies based on the wireless channel reciprocity [5], secure coding technologies based on the different wireless channel states, such as Low Density Parity Check Code(LDPC) [6]. For a jamming scene with one transmitter, one legitimate receiver and one jammer, the major physical layer security method is the anti-jamming technology based on beamforming [7]. However, when combining two scenarios, the simultaneous presence of the eavesdropper and jammer can significantly reduce the system secrecy rate. The jammer (malicious jammer relay) would jam the legitimate receiver by sending noise, or cooperate with the eavesdropper by sending linear source signals. In this case, the existing physical layer security approaches are no longer applicable. New targeted physical layer security technologies should be proposed, which needs of detail performance analysis. According to a four-node network with one transmitter, one legitimate receiver, one eavesdropper and one malicious jammer relay helping the eavesdropper, secure performance affected by the malicious jammer relay is analyzed through means of amplify-and-forward, decode-and-forward and compress-and-forward in [8]. Source signals are assumed to be known by malicious jammer relay in [9], this paper establishes the malicious jammer relay and transmitter as a zero-sum game model with the objective function of secrecy rate. Then, it analyzes the achievable balanced performance between malicious jammer relay and transmitter due to the constraint relationship. In [10], a supplementary analysis that the transmitter and malicious jammer relay can select the appropriate rate to send signals or noise to increase or reduce secrecy rate is offered, respectively. In the literatures of the scene with both eavesdropping and jammer, threats caused by a single malicious jammer relay are studied. However, in reality scenes, there may be several malicious jammer relays, and the impact on system performance caused by their cooperation is lack of analysis.

To cope with the problem, we establish a complex Gaussian network model firstly, which includes one transmitter, one legitimate receiver, one eavesdropper and several malicious jammer relays assisting the eavesdropper. These malicious jammer relays eavesdrop the signal from the transmitter and

Shengbin Lin is a student of National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China.

Qingfeng Liu is the associate professor of National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China.

Kaizhi Huang is the director of mobile communication department for National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China (corresponding author to provide phone: 0371-81632766; e-mail: realbinforever@163.com).

then cooperate to transmit linear amplification of the eavesdropping signals and noise to reduce system secrecy rate according to their channel states with power constraint. At the same time, due to the different noise, we deduce secrecy rate on Gaussian noise and structured noise scenarios. Finally, simulation results analyze the performance of physical layer security under the cooperation of multiple malicious jammer relays.

The rest of the paper is organized as follows: Section II describes the system model of the complex Gaussian network. In Section III, the security performance of multiple malicious jammer relays is analyzed in both Gaussian noise and structured noise scenarios. The simulation results are carried out in Section IV. Finally in Section V, some conclusions are drawn.

II. Network Modeling

Consider a complex Gaussian network model consisted of one transmitter, one legitimate receiver, one eavesdropper and several malicious jammer relays assisting the eavesdropper, as shown in Fig. 1. As all malicious jammer relays eavesdrop the source signals first, the received signals at the legitimate receiver, eavesdropper and malicious jammer relays can be expressed as

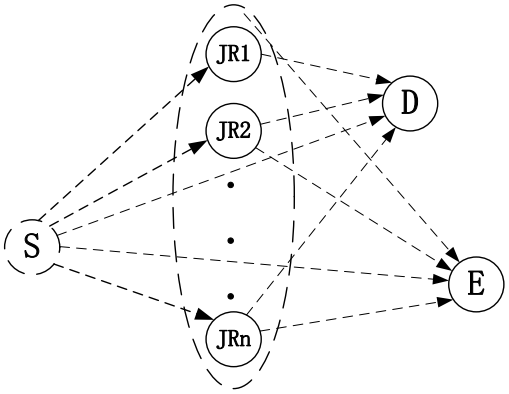

Fig. 1 Complex Gaussian network model. S: Sender, D: Destination, E: Eavesdropper, JR: Jamming Relay

$$Y_{D,i} = h_{SD} X_{S,i} + \sum_{j=1}^{n} h_{R_j D} X_{R_j,i} + Z_{D,i} \tag{1}$$

$$Y_{E,i} = h_{SE} X_{S,i} + \sum_{j=1}^{n} h_{R_j E} X_{R_j,i} + Z_{E,i} \tag{2}$$

$$Y_{R_j,i} = h_{SR_j} X_{S,i} + Z_{R_j,i} \tag{3}$$

Where $X_{S,i}$ and $X_{R_j,i}$ respectively represent the signals transmitted by transmitter and j-th $j, j = 1,...,n$ jamming relay in time $i, i = 1,...,t$. There are jamming relay n jamming relay in all. $h_{k,l}$, $k = S, R_j$, $l = R_j, D, E$ denotes the complex channel gain between node k and l. Considering the worst circumstance, we assume that all the channel gains are available to the malicious jammer relays. $Z_{D,i}$, $Z_{E,i}$ and $Z_{R_j,i}$ are independent complex additive Gaussian noise at the legitimate receiver, eavesdropper and j-th relay with zero-mean and variance $N_D = N_E = N_0$, $N_{R_j} = N_1$, respectively. At the same time, P_S and P_R are the power constraint at the transmitter and the malicious jammer relays.

Due to power constraint, all malicious jammer relays cooperate to transmit linear amplification of the eavesdropping signals and noise to reduce secrecy rate according to their channel states. We assume that signals sent by transmitter and malicious jammer relays can simultaneously reach legitimate receiver and eavesdropper, respectively. Thus, the jamming signal $X_{R_j,i}$ at the j-th relay is given by:

$$X_{R_j,i} = \rho_j Y_{R_j,i} + Z_{j,i} \tag{4}$$

Where $\rho_j \in \square$ represents the linear coefficient of eavesdropping signals. It is of great importance for the malicious jammer relays to send the part of $\rho_j Y_{R_j,i}$. As $Y_{R_j,i}$ contains $h_{SR_j} X_{S,i}$, the j-th relay would send the parameter of $\rho_j h_{SR_j} X_{S,i}$, which equals linear source signal. In this way, the malicious jammer relays can simultaneously decrease or increase the SNR at the legitimate receiver and eavesdropper. However, the increasing or decreasing degrees are different due to the different channel states. By setting appropriate ρ_j, the malicious jammer relays are able to deteriorate the communication and finally decrease the secrecy rate.

$Z_{j,i}$ is noise independent of $X_{R_j,i}$ and can be Gaussian noise or structured noise. The function of noise is similar to the former signal. When $Z_{j,i}$ is Gaussian noise, both the legitimate receiver and eavesdropper will be interfered. However the interferences at the legitimate receiver and eavesdropper are not the same owing to the different path loss. When $Z_{j,i}$ is structured noise, the eavesdropper cooperating with malicious jammer relays knows the noise in advance and can remove the noise from received signals

III. Security Performance Of Multiple Malicious Jammer Relays

A. When $Z_{j,i}$ is Gaussian noise

Noise transmitted by malicious jammer relays is divided into two categories, which will be analyzed separately. When the noise is Gaussian noise, from formula (1), (2), (3) and (4), we can get the signals of legitimate receiver and eavesdropper as following:

$$\tilde{Y}_{D,i} = X_{S,i} + \tilde{Z}_{D,i} \tag{5}$$

$$\tilde{Y}_{E,i} = X_{S,i} + \tilde{Z}_{E,i} \tag{6}$$

where,

$$\tilde{Z}_{D,i} = \frac{\sum_{j=1}^{n}\left(h_{R_jD}\rho_j Z_{R_j} + h_{R_jD}Z_{j,i}\right) + Z_{D,i}}{\sum_{j=1}^{n} h_{SR_j}h_{R_jD}\rho_j + h_{SD}} \quad (7)$$

$$\tilde{Z}_{E,i} = \frac{\sum_{j=1}^{n}\left(h_{R_jE}\rho_j Z_{R_j} + h_{R_jE}Z_{j,i}\right) + Z_{E,i}}{\sum_{j=1}^{n} h_{SR_j}h_{R_jE}\rho_j + h_{SE}} \quad (8)$$

As $Z_D, Z_E \sim CN(0, N_0)$, the variances of $\tilde{Z}_{D,i}$ and $\tilde{Z}_{E,i}$ are:

$$\tilde{N}_{D,i} = \frac{\sum_{j=1}^{n}\left(\left|h_{R_jD}\rho_j\right|^2 N_{Z_{R_j}} + \left|h_{R_jD}\right|^2 N_{Z_j}\right) + N_0}{\left|\sum_{j=1}^{n} h_{SR_j}h_{R_jD}\rho_j + h_{SD}\right|^2} \quad (9)$$

$$\tilde{N}_{E,i} = \frac{\sum_{j=1}^{n}\left(\left|h_{R_jE}\rho_j\right|^2 N_{Z_{R_j}} + \left|h_{R_jE}\right|^2 N_{Z_j}\right) + N_0}{\left|\sum_{j=1}^{n} h_{SR_j}h_{R_jE}\rho_j + h_{SE}\right|^2} \quad (10)$$

From formula (5) and (6), the system equals to a Gaussian wiretap channel model. The transmitter will transmit Gaussian codebook with total power to maximize its secrecy rate [11]:

$$R_S(\rho_1,..,\rho_n,N_{Z_1},...,N_{Z_n}) = [\log_2(1+\frac{P_S}{\tilde{N}_D}) - \log_2(1+\frac{P_S}{\tilde{N}_E})]^+ \quad (11)$$

Since transmitter transmits complex Gaussian signals and all the malicious jammer relays allocate power by cooperation and select appropriate ρ_j and $N_{Z_{R_j}}$ to minimize the secrecy rate. The goal of the malicious jammer relays can be converted into the optimization problem as following:

$$\begin{aligned} &\min R_S(\rho_1,..,\rho_n,N_{Z_1},...,N_{Z_n}) \\ &\text{s.t.} \sum_{j=1}^{n}\left(\left|\rho_j h_{SR_j}\right|^2 P_S + \left|\rho_j\right|^2 N_{R_j} + N_{Z_j}\right) \le P_R \end{aligned} \quad (12)$$

We assume that $R_S^*(\rho_1^*,...,\rho_n^*,N_{Z_1}^*,...,N_{Z_n}^*)$ is the minimum secrecy rate, and $\rho_j^*, N_{Z_j}^*$ are the value of ρ_j and N_{Z_j}, respectively.

It is obvious to find the formula (11) is not a convex function. Although there is no general solution, we can get the following conclusion in some specific cases:

(1)When $|h_{SE}| \ge |h_{SD}|$, i.e. the eavesdropping channel is better than the legitimate channel. Without the help of malicious relay, the secrecy rate is already zero. So there is no need for malicious relay to transmit any jamming signals.

(2)When $\max(|h_{SR_1}h_{R_1D}|,...,|h_{SR_n}h_{R_nD}|) \ge \sqrt{P_S/(P_R-N_1)}\,|h_{SD}|$, malicious relay can transmit negative linear signals to eliminate source signals at the legitimate receiver.

(3)When $\max(|h_{SR_1}h_{R_1D}|,...,|h_{SR_n}h_{R_nD}|) < \sqrt{P_S/(P_R-N_1)}\,|h_{SD}|$ and $|h_{SE}| \le |h_{SD}|$, the malicious relay cannot just transmit linear signals or noise to make the system secrecy rate zero. The channel state information is shared by all of the malicious relays, so they will allocate the jamming power cooperatively. An appropriate jamming coefficient and noise power will be set to minimize the secrecy rate of the system. We can solve the problem using numerical simulation. In (12), it can be shown that the constraint is not necessarily met with equality; i.e., there is no need for the malicious jammer relays to use total jamming power. When $\rho_j = |\rho_j|e^{j\theta_j}$, $N_{Z_j} = \omega_j P_S$, the constraint condition can be converted as

$$\begin{aligned} &\sum_{j=1}^{n} P_{R_j} = P_R \\ &|\rho_j| \le \sqrt{(P_{R_j}-N_1)/P_S} \\ &0 \le \theta_j \le 2\pi \\ &0 \le \omega_j \le P_{R_j}/P_S - |\rho_j|^2 \end{aligned} \quad (13)$$

We traverse the values of $|\rho_1|,...,|\rho_n|$, $\theta_1,...,\theta_n$, and $\omega_1,...,\omega_n$, and get the minimum value of the objective function. From the process of numerical analysis, we can notice that the calculation significantly increases with additional three parameters as a result of an added relay.

B. When $Z_{j,i}$ is structured noise

As malicious jammer relays cooperate with eavesdropper, the eavesdropper is able to know the structured noise in advance so that it can remove the noise from the received signal. In this case, the signal received by eavesdropper becomes

$$\bar{Y}_{E,i} = X_{S,i} + \bar{Z}_{E,i} \quad (14)$$

Where,

$$\bar{Z}_{E,i} = \frac{Z_{E,i}}{(\sum_{j=1}^{n} h_{SR_j}h_{R_jE}\rho_j + h_{SE})} \quad (15)$$

Variance is $\bar{N}_E$

$$\bar{N}_{E,i} = \frac{N_0}{\left|\sum_{j=1}^{n} h_{SR_j} h_{R_j E} \rho_j + h_{SE}\right|^2} \quad (16)$$

However, the legitimate receiver does not know the structure of noise. In this case, the transmitter sends a Gaussian codebook with total power to maximize secrecy rate with full power.

$$\bar{R}_S(\rho_1,..,\rho_n,N_{Z_1},...,N_{Z_n}) = [\log 2(1+\frac{P_S}{\tilde{N}_D}) - \log 2(1+\frac{P_S}{\bar{N}_E})]^+ \quad (17)$$

Comparing $\tilde{N}_E$ and $\bar{N}_E$ received by eavesdropper in the two scenarios, we can conclude that the secrecy rate of sending structured noise is less than that sending Gaussian noise.

Fig. 2 shows the diversification curves of secrecy rate under the structured noise and Gaussian noise in fixed channel. The two curves have similar envelopes: when $|h_{RE}|$ is relatively large, i.e. the channel states between malicious jammer relays and eavesdropper are good, the two kinds of noise can both decrease system secrecy rate. When the channel states between malicious jammer relays and eavesdropper are poor, relay cannot effectively decrease secrecy rate down to zero, then the performance of sending structured noise is better than that of sending Gaussian noise. However, structured noise needs that eavesdropper and relays share structured codebook in advance, while the design of Gaussian noise system is relatively simple.

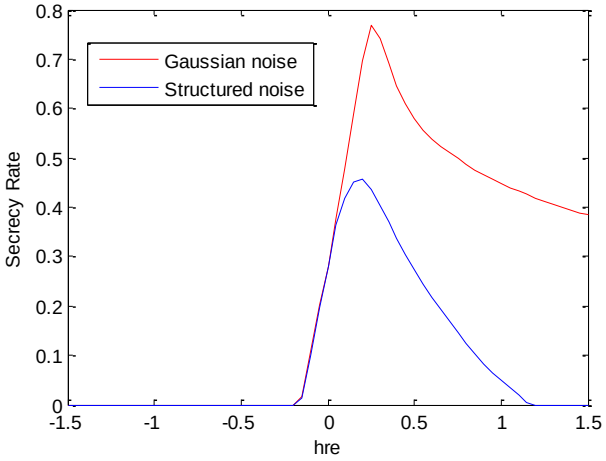

Fig. 2 Secrecy rate under different types of noise

In this case, the target of malicious jammer relays is also converted into the optimization problem with the same power constraint

$$\begin{aligned} &\min \bar{R}_S(\rho_1,..,\rho_n,N_{Z_1},...,N_{Z_n}) \\ &\text{s.t.} \sum_{m=1}^{n}\left(\left|\rho_m h_{SR_m}\right|^2 P_S + \left|\rho_m\right|^2 N_{R_m} + N_{Z_m}\right) \le P_R \end{aligned} \quad (18)$$

We draw the following similar conclusions

(1)When $|h_{SE}| \ge |h_{SD}|$, the secrecy rate is already zero even the malicious jammer relays keep silent.

(2)When $\max(|h_{SR_1} h_{R_1 D}|,...,|h_{SR_n} h_{R_n D}|) \ge \sqrt{P_S/(P_R - N_1)}\,|h_{SD}|$, $(\rho^*, N_Z^*) = (-h_{SD}/\max(h_{SR_1} h_{R_1 D},...,h_{SR_n} h_{R_n D}),0)$ is the optimal.

(3)When $\max(|h_{SR_1} h_{R_1 D}|,...,|h_{SR_n} h_{R_n D}|) < \sqrt{P_S/(P_R - N_1)}\,|h_{SD}|$ and $|h_{SE}| \le |h_{SD}|$, we also use numerical simulation methods to find the minimum value of the objective function.

IV. Simulation Results And Security Analysis

In this section, we carry out some simulation results to analyze the influence of cooperative multiple malicious jammer relays on secrecy rate. As mentioned above, the computation significantly increases with the increasing of relay number. For simplicity, the number of malicious jammer relays is set 2 during the simulation. We also normalize the channel gains and fix $h_{SD} = 1$, $h_{SE} = 0.4 + 0.4j$, $h_{R_1 D} = 0.2 - 0.2j$, $h_{R_2 D} = 0.3 + 0.1j$, $h_{SR_1} = 0.5 + 0.5j$, $h_{SR_2} = 0.4 - 0.4j$, $P_S = P_R = 10$, $N_0 = 1$. The figures' x-axis h_{RE} denoting the channel state between the jammer relay and the eavesdropper is ranged as real.

The existing literature generally assume that the malicious jammer relay knows the source signal. However, this paper allows the malicious jammer relays to eavesdrop the source signal first and then a jamming signal based on the eavesdropping signal and noise is sent. Fig. 3 describes the secrecy rate curve under both conditions of malicious jamming relay knowing the source signal and jamming based on eavesdropping signal. We can conclude that the scene of knowing the source signal reduce the secrecy rate more under the same power constraint. This is due to the eavesdropping signal contains both source signal and Gaussian noise. When the malicious jammer relays intend reducing the secrecy rate by sending a negative linear amplification of the eavesdropping signal, he must send the accompanying Gaussian noise with additional power consumption, which is not expected by the malicious jammer relays. When the source signal is known, he can independently send a negative linear source signal without carrying any additional noise. This is actually a special case of the former scene. When $Z_{R_j,i}$ in the formula (3) is zero, the jamming scene based on eavesdropping signal equals to the scene that the source signal is known.

Fig. 4 shows the secrecy rate under different SNRs when jamming based on eavesdropping signal. Under the same noise type, we can see that when the SNR of the eavesdropping signal is large, i.e. the value N_1 is small, the secrecy rate is reduced effectively. With the increasing of N_1, the noise part in the eavesdropping signal becomes larger, which increases the relevance between the source signal and Gaussian noise so that the jamming ability decreases under the power constraint.

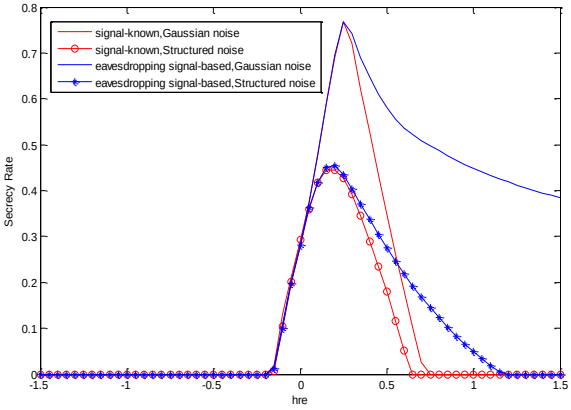

Fig. 3 The secrecy rate curve under both condition of knowing the source signal and jamming based on eavesdropping signal

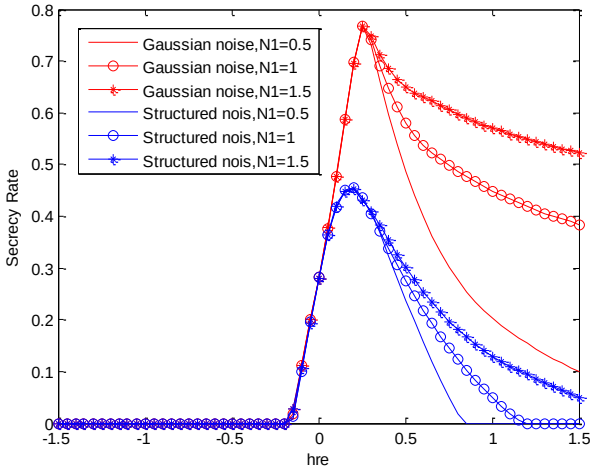

Fig. 4 The secrecy rate curve under different SNR of the eavesdropping signal

According to the channel states, the multiple malicious jammer relays cooperate allocating the jamming power and sending the appropriate linear amplification of the eavesdropping signal and noise to effectively reduce the secrecy rate. Fig. 5 and 6 both describe the secrecy rate in conditions of two malicious jamming relays are separate and cooperative. Seen from Fig. 5, the jamming performance of cooperation between two malicious jammer relays is better with the same power constraint. The average secrecy rate of cooperation relay is 0.15bits/s/Hz less than that of one relay under Gaussian noise, and the average secrecy rate of cooperation relay is 0.05bits/s/Hz less than that of one relay under structured noise.

Fig. 6 analyzes the cooperation performance of two malicious jammer relays under both conditions of knowing the source signal and jamming based on eavesdropping signal. When two malicious jammer relays cooperate jamming based on the eavesdropping signal, the secrecy rate before the peak is lower than that in the condition of a single malicious jammer relay knowing the source signal, however, slightly larger after the peak rate. When two malicious jammer relays cooperate in case of knowing the source signal, the secrecy rate before the peak is similar to that in the condition of cooperating jamming based on the eavesdropping signal and almost coincide to that the condition of a single malicious jammer relay knowing the source signal after the peak rate.

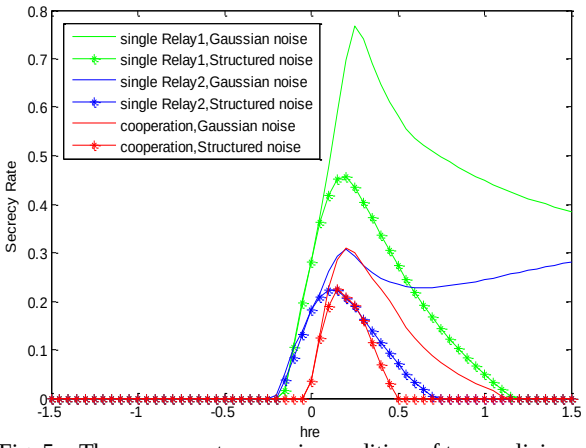

Fig. 5 The secrecy rate curve in condition of two malicious jamming relays are separate and cooperative

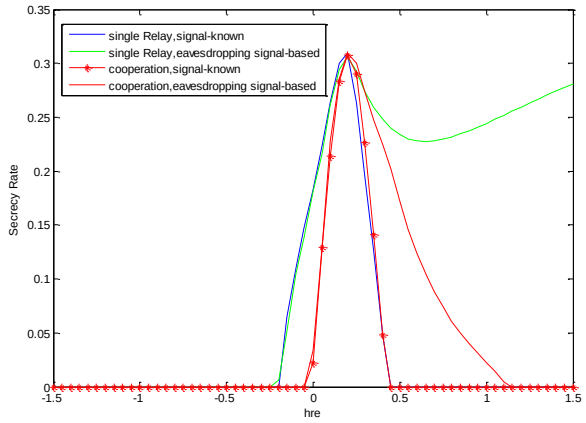

Fig. 6 The secrecy rate curve in conditions of two malicious jamming relays are separate and cooperative using Gaussian noise.

V. Conclusion

In this paper, we analyze physical layer security performance under the cooperation of multiple malicious jammer relays. Firstly, we create a complex Gaussian model, containing multiple malicious jammer relays which cooperate with the eavesdropper, and have no knowledge of the source signal. After eavesdropping the source signal, these malicious jammer relays send linear amplification of the eavesdropping signal and noise according to their channel state in the limited power by cooperation, so that eavesdropper can reduce system secrecy rate by cooperation with relay. Finally, numerical simulations show the different results between multiple malicious jammer relays and a single malicious jammer relay.

References

[1] P. Gupta and P. Kumar, "The capacity of wireless networks", *IEEE Transaction on Information Theory*, vol. 46, no. 2, pp. 388-404, 2000.

[2] A. D. Wyner, "The wire-tap channel", *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[3] M. Bloch and M. Debbah, "Special issue on physical-layer security", *Journal of Communications and Networks*, vol. 14, no. 4, pp. 349-351, 2012.

[4] P. H. Lin and S. H. Lai, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels", *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728-1740, 2013.

[5] T. H. Chou and S. C. Draper, "Secret key generation from sparse wireless channels: ergodic capacity and secrecy outage", *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1751-1764, 2013.
[6] G. Dziwoki and W. Sulek, "Subchannel ordering scheme for LDPC-coded OFDM transmission over selective channels", *International Conference on Telecommunications and Signal Processing*, 2013: 66-70.
[7] X. H. Wang and X. W. Shi, "Smart antenna design for GPS/GLONASS anti-jamming using adaptive beamforming", *IEEE International Conference on Microwave and Millimeter Wave Technology*, 2010: 1149-1152.
[8] M. Yuksel, and E. Erkip, "Secure communication with a relay helping the wire-tapper", *IEEE Information Theory Workshop*, 2007: 595-600.
[9] M. Yuksel, and E. Erkip, "A secrecy game with an informed jammer relay", *IEEE International Symposium on Personal Indoor and Mobile Radio Communications*, 2010: 2687-2691.
[10] M. Yuksel, and E. Erkip, "A secure communication game with a relay helping the eavesdropper", *IEEE Transaction on Information Forensics and Security*, vol. 6, no. 3, pp. 818-830, 2011.
[11] A. Kashyap, T. Basar, "Correlated jamming on MIMO Gaussian fading channels", *IEEE Transaction on Information Theory*, vol. 50, no. 9, pp. 2119-2123, 2004

Qingfeng Liu is currently the associate professor of National Digital Switching System Engineering & Technological Research Center. His research interests include wireless mobile communication network and physical layer security.

Kaizhi Huang received the Ph.D. degree in communication and information system from Tsinghua University. She is currently a professor and supervisor of Ph.D. student. Now, she is the director of mobile communication department for National Digital Switching System Engineering & Technological Research Center. Her research interests include wireless mobile communication network and information secrecy.