Trade-off Performance Analysis and System Optimization of Opportunistic Relaying Cooperative Communication Systems over Nakagami-m Fading Channels: Postprint

Authors: Peng Lei, Zang Guozhen, Gao Yuanyuan, Sha Nan, Jiang Xuanyou

Date: 2018-10-11T00:00:00+00:00

Abstract

To address the security threats posed by external eavesdroppers to information transmission in multi-relay cooperative communication systems, a cooperative secure transmission scheme is proposed wherein relay nodes transmit artificial jamming signals while forwarding information. The security performance of this scheme in Nakagami-m fading channels is analyzed, and closed-form expressions for the outage probability and intercept probability—used to evaluate the reliability and security of opportunistic relaying systems, respectively—are derived. Based on these expressions, the trade-off performance of the system is discussed from both reliability and security perspectives. Simulations verify the correctness of the derivations and clarify the impact of the number of relays on the system' s trade-off performance. Finally, to further improve the system' s trade-off performance, the power allocation problem between artificial jamming signals and communication signals is discussed, and the power allocation factor that optimizes the system' s trade-off performance is obtained through simulations.

Full Text

Preamble

Tradeoff Performance Analysis and System Optimization of Opportunistic Relay Cooperative Communication System under Nakagami-m Fading Channel

Peng Lei, Zang Guozhen, Gao Yuanyuan, Sha Nan, Jiang Xuanyou
(College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China)

Abstract: To address the security threats posed by external eavesdroppers to information transmission in multi-relay cooperative communication systems, this paper proposes a cooperative secure transmission scheme where relay nodes forward information while simultaneously transmitting artificial interference signals. The security performance of this scheme under Nakagami-m fading channels is analyzed, and closed-form expressions for outage probability (representing system reliability) and intercept probability (representing system security) are derived for opportunistic relay systems. Based on these results, the tradeoff performance of the system is discussed from both reliability and security perspectives. Simulations verify the correctness of the derivations and clarify the impact of the number of relays on the system' s tradeoff performance. Finally, to further improve the system' s tradeoff performance, the paper also discusses the power allocation problem between artificial interference signals and communication signals, and obtains the optimal power allocation factor that maximizes the system' s tradeoff performance through simulation.

Key words: cooperative communication; Nakagami-m fading channel; relay selection; outage probability; intercept probability

0 Introduction

With the rapid development and widespread application of wireless communication technology, the demand for data services continues to grow, accompanied by increasingly stringent requirements for the confidential transmission of personal private information. Cooperative communication leverages collaborative information processing among nodes within the system to achieve excellent diversity gains, thereby effectively improving the reliability of information transmission [1]. Due to its superior anti-fading performance, cooperative communication technology has been extensively studied in the wireless communication field [2,3]. However, because of the openness of wireless channels and the broadcast nature of information transmission, cooperative communication increases the risk of information being intercepted by eavesdroppers while improving transmission reliability and expanding communication range.

In recent years, physical layer security technology has gained widespread attention as a complement to traditional encryption techniques, with artificial interference being a common method for implementing physical layer security that has found extensive application in addressing security threats to cooperative communication systems [4,5]. Reference [4] presents a secure communication scheme where the source node transmits artificial interference signals and optimizes the allocation of total transmit power to achieve optimal security performance. Reference [5] utilizes artificial interference to enhance the security of two-way relay communication systems, designing precoding matrices for relays and users to effectively prevent information interception by eavesdroppers.

Currently, research on cooperative communication systems primarily focuses on single performance metrics such as reliability or security. However, practical

applications require attention to comprehensive system performance. Recently, the industry has begun investigating the combined performance of cooperative communication systems in terms of both reliability and security [6,7] to make them more applicable in real-world scenarios. Reference [6] first introduced the concept of secrecy outage probability, opening new avenues for system security analysis. Reference [7] analyzed the reliability and security of opportunistic relay cooperative communication systems under Rayleigh fading channels. Through numerical simulations of outage probability (representing reliability) and intercept probability (representing security), it was found that improvements in information transmission reliability in cooperative communication systems are accompanied by decreases in security, and vice versa. However, practical systems typically desire both optimal reliability and security, a consideration not addressed in that work regarding the system' s comprehensive performance.

Relay nodes are unique to cooperative communication systems, and system performance generally varies depending on which node is selected as the relay. Consequently, relay selection has always been a critical aspect of cooperative communication system design and has been widely studied in the industry [8,9]. Reference [8] employs a maximum SNR strategy for relay selection and analyzes the system' s outage probability and diversity gain. Reference [9] proposes optimal and suboptimal relay selection schemes depending on whether the eavesdropping channel state information is known, and derives asymptotic closed-form expressions for secrecy outage probability under both schemes. However, these studies also investigate relay selection in the system based on single performance aspects of reliability or security, without considering the system' s comprehensive performance.

This paper proposes a secure transmission scheme for a multi-relay cooperative communication system model in the presence of eavesdroppers, where opportunistic relays forward information while simultaneously transmitting artificial interference. Based on the more general Nakagami-m fading channel, a tradeoff analysis of the system' s reliability and security is conducted. Closed-form expressions for the outage probability of the main channel (representing reliability) and the intercept probability of the eavesdropping channel (representing security) are first derived. These two probabilities are then considered as a whole to analyze the tradeoff performance of the system in terms of both information transmission reliability and security. Simulations verify the correctness of the derivations and analyze the impact of the number of relays on system security performance. Finally, the power allocation problem between artificial interference and source signals is discussed, and the power allocation factor that optimizes the system' s tradeoff performance is obtained.

1 System Model

The system model considered in this paper is shown in [Figure 1: see original paper]. In the presence of an eavesdropper E, the system comprises a single source S, a destination D, and N relays (where $|\mathcal{R}| = N$ represents the cardinality of set

$\mathcal{R}$). There are no direct links between S and D or between S and E due to long distances, while both D and E are within the communication coverage range of the relays. Therefore, when relays forward information to D, E can also receive the forwarded information. All relay nodes operate in half-duplex mode and employ a decode-and-forward cooperative strategy. Each node is equipped with a single antenna for transmitting and receiving information. During communication, the system adopts an opportunistic relay strategy, selecting only one relay to forward source information to destination D. To degrade the eavesdropping channel quality, the selected relay is assumed to transmit D-known artificial interference signals (such as pseudo-random sequences) along with the source information to reduce the SINR at E. All links are assumed to be Nakagami-m fading channels. The meanings of commonly used symbols in the paper are listed in .

The entire information transmission process can be divided into two phases. In the first phase, S transmits source information to all relays. Due to differences in channel conditions between S and each R_k, not all signals received by the relays can meet the requirements for perfect decoding and forwarding. For analytical convenience, let $\mathcal{D}$ denote the set of relays that can successfully decode. When $\mathcal{D}$ is empty, it indicates that no relay can decode the source information; when $\mathcal{D}$ equals the full set $\mathcal{R}$ (i.e., $|\mathcal{D}| = |\mathcal{R}| = N$), it means all relays can achieve perfect decoding.

In the first phase, the signal received at relay R_k can be expressed as:

$$y_{R_k} = \sqrt{P_S} h_{SR_k} x + n_{R_k}$$

where P_S represents the transmit power of S, h_{SR_k} denotes the channel fading coefficient between S and the k-th relay following a Nakagami-m distribution, x is the source signal, and n_{R_k} represents the additive white Gaussian noise (AWGN) at the relay with zero mean and variance $\sigma^2_{R_k}$, i.e., $n_{R_k} \sim \mathcal{CN}(0, \sigma^2_{R_k})$. Therefore, using Shannon' s theorem, the channel capacity between S and R_k can be obtained as:

$$C_{SR_k} = \frac{1}{2} \log_2 \left(1 + \frac{P_S |h_{SR_k}|^2}{\sigma^2_{R_k}} \right)$$

where the factor $\frac{1}{2}$ indicates that information transmission occupies two time slots.

Let $\gamma_{ij} = |h_{ij}|^2$ denote the channel gain, where γ_{ij} follows a gamma distribution, i.e., $\gamma_{ij} \sim \text{Gam}(m_{ij}, \lambda_{ij})$. Here, m_{ij} is the Nakagami shape factor representing the fading severity due to scattering and multipath interference processes, and λ_{ij} represents the average power of multipath scattering components, with its probability density function given by:

$$f_{\gamma_{ij}}(\gamma) = \frac{\lambda_{ij}^{m_{ij}} \gamma^{m_{ij}-1}}{\Gamma(m_{ij})} e^{-\lambda_{ij}\gamma}$$

In the second phase, if the decoding relay set $\mathcal{D}$ is not empty, the forwarded information from one relay in this set will serve as the decoded signal for destination D. The relay selection strategy in this paper chooses the relay that maximizes the channel coefficient between the relay and D, i.e.:

$$R^* = \arg \max_{R_k \in \mathcal{D}} |h_{R_{kD}}|^2$$

where $|h_{R_{kD}}|^2$ represents the channel gain between the k-th relay and D. This relay selection strategy only requires knowledge of the main channel' s channel state information (CSI) and does not require knowledge of the eavesdropping channel state information.

The selected relay R^* decodes the information from S, re-encodes it, and forwards it while simultaneously transmitting D-known artificial interference signals. The signals received at the destination and the eavesdropper can be expressed respectively as:

$$y_D = \sqrt{P_R} h_{R^*D} x + \sqrt{P_J} h_{R^*D} x_J + n_D$$

$$y_E = \sqrt{P_R} h_{R^*E} x + \sqrt{P_J} h_{R^*E} x_J + n_E$$

where P_R and P_J are the relay' s forwarding power and interference transmit power, respectively; x and x_J represent the forwarded source signal and artificial interference signal, respectively; and n_D and n_E denote the additive white Gaussian noise received at the destination and eavesdropper, respectively.

Assuming destination D knows the CSI of the main channel and the artificial interference sent by the relay, it can completely eliminate the impact of artificial interference on decoding. In contrast, eavesdropper E has no knowledge of the artificial interference. Therefore, the channel capacities of the selected relay R^* to D and E can be expressed as:

$$C_{R^*D} = \frac{1}{2} \log_2 \left(1 + \frac{P_R |h_{R^*D}|^2}{\sigma_D^2} \right)$$

$$C_{R^*E} = \frac{1}{2} \log_2 \left(1 + \frac{P_R |h_{R^*E}|^2}{P_J |h_{R^*E}|^2 + \sigma_E^2} \right)$$

Let $\gamma_{R^*D} = |h_{R^*D}|^2$ and $\gamma_{R^*E} = |h_{R^*E}|^2$, both of which follow gamma distributions, i.e., $\gamma_{R^*D} \sim \text{Gam}(m_{R^*D}, \lambda_{R^*D})$ and $\gamma_{R^*E} \sim \text{Gam}(m_{R^*E}, \lambda_{R^*E})$.

2 System Performance Analysis

This section derives closed-form expressions for the outage probability (OP, representing system reliability) and intercept probability (IP, representing system security) of the proposed system scheme in Nakagami fading channels. A performance metric that includes both OP and IP is then defined to analyze the

tradeoff performance (SRT) of the system as a whole [10]. Finally, the impact of power allocation among various signals in the system on system performance is analyzed.

In physical layer security, the source encoder typically needs to design codes that maximize both the data rate at the legitimate destination D (R_D) and the equivocation rate at eavesdropper E (R_E). If the data rate equals the equivocation rate ($R_D = R_E$), perfect security can be achieved, meaning D can achieve a data rate of R_D while the mutual information between S and E is zero [7]. Therefore, in the following analysis, the same threshold value R_S is used for both outage probability and intercept probability.

2.1 Outage Probability (Reliability)

Based on the channel capacities derived above for relay nodes and the destination node, for a given target transmission rate R_S, the outage probability (OP) of system information transmission can be defined as the probability of the outage event $\{C_{SD} < R_S\}$ [7], which measures the reliability of information transmission in communication systems. Therefore, using the law of total probability, the OP expression is obtained as:

$$P_{\text{out}} = \sum_{n=0}^{N} \Pr\{\mathcal{D} = \mathcal{D}_n\} \Pr\{C_{SD} < R_S | \mathcal{D} = \mathcal{D}_n\}$$

where R_S is the data transmission rate and $\mathcal{D}_n$ represents a relay subset.

When $\mathcal{D} = \emptyset$, it means $\Pr\{\mathcal{D} = \mathcal{D}_0\}$, and no relay forwards information to D. Therefore, equation (9) can be rewritten as:

$$P_{\text{out}} = \Pr\{\mathcal{D} = \emptyset\} + \sum_{n=1}^{N} \Pr\{\mathcal{D} = \mathcal{D}_n\} \Pr\{C_{R^*D} < R_S | \mathcal{D} = \mathcal{D}_n\}$$

$\Pr\{\mathcal{D} = \mathcal{D}_n\}$ represents the probability that n relays can successfully decode the source information. Combining with equation (2), we obtain:

$$\Pr\{\mathcal{D} = \mathcal{D}_n\} = \Pr\{C_{SR_i} > R_S, i \in \mathcal{D}_n\} \Pr\{C_{SR_j} < R_S, j \in \bar{\mathcal{D}}_n\}$$

where $\bar{\mathcal{D}}_n$ is the complement of $\mathcal{D}_n$, and $|\mathcal{D}_n| = n$. Similarly, $\Pr\{C_{R^*D} < R_S | \mathcal{D} = \mathcal{D}_n\}$ can be calculated as:

$$\Pr\{C_{R^*D} < R_S | \mathcal{D} = \mathcal{D}_n\} = \Pr\left\{\frac{1}{2}\log_2\left(1 + \frac{P_R \gamma_{R^*D}}{\sigma_D^2}\right) < R_S\right\}$$

From equations (4) and (7), it can be observed that when the impact of artificial interference on the legitimate receiver is ignored, selecting the relay that

maximizes the channel gain from relay k to D is equivalent to selecting the relay that maximizes channel capacity, i.e.:

$$R^* = \arg \max_{R_k \in \mathcal{D}} C_{R_{kD}}$$

Substituting equations (11), (12), and (14) into (10) yields the closed-form expression for OP:

$$P_{\text{out}} = \Phi_1^N + \sum_{n=1}^{N} \binom{N}{n} \Phi_1^{N-n} (1-\Phi_1)^n \Phi_2$$

where $\Phi_1 = \Pr\{\gamma_{SR_k} < \Lambda_1\}$, $\Phi_2 = \Pr\{\gamma_{R^*D} < \Lambda_2\}$, and $\Lambda_1 = \frac{2^{2R_S}-1}{P_S/\sigma^2_{R_k}}$, $\Lambda_2 = \frac{2^{2R_S}-1}{P_R/\sigma^2_D}$. Based on the derivation in Appendix A, the closed-form expressions are:

$$\Phi_1 = \frac{1}{\Gamma(m_{SR_k})} \sum_{i=0}^{\infty} \frac{(-1)^i \lambda_{SR_k}^{m_{SR_k}+i} \Lambda_1^{m_{SR_k}+i}}{i!(m_{SR_k}+i)}$$

$$\Phi_2 = \frac{1}{\Gamma(m_{R^*D})} \sum_{i=0}^{\infty} \frac{(-1)^i \lambda_{R^*D}^{m_{R^*D}+i} \Lambda_2^{m_{R^*D}+i}}{i!(m_{R^*D}+i)}$$

2.2 Intercept Probability (Security)

Similarly, the intercept probability (IP) can be defined as the probability of the intercept event $\{C_{SE} > R_S\}$, which measures the security of information transmission in communication systems [7]. For the proposed system model, the occurrence of an intercept event requires that at least one relay can correctly decode, i.e., $\mathcal{D} \neq \emptyset$. Therefore, IP can be expressed as:

$$P_{\text{int}} = \Pr\{C_{SE} > R_S, \mathcal{D} \neq \emptyset\}$$

Expanding the conditional probability using the law of total probability yields:

$$P_{\text{int}} = \sum_{n=1}^{N} \Pr\{\mathcal{D} = \mathcal{D}_n\} \Pr\{C_{R^*E} > R_S | \mathcal{D} = \mathcal{D}_n\}$$

where $\Pr\{\mathcal{D} = \mathcal{D}_n\}$ is given by equation (11). The conditional probability can be calculated as:

$$\Pr\{C_{R^*E} > R_S | \mathcal{D} = \mathcal{D}_n\} = \Pr\left\{\frac{1}{2}\log_2\left(1 + \frac{P_R \gamma_{R^*E}}{P_J \gamma_{R^*E} + \sigma_E^2}\right) > R_S\right\}$$

Let $\Lambda_3 = \frac{2^{2R_S}-1}{P_R/\sigma_E^2 - 2^{2R_S} P_J/\sigma_E^2}$. When $P_R/\sigma_E^2 > 2^{2R_S} P_J/\sigma_E^2$, we have $\Lambda_3 > 0$, and:

$$\Pr\{C_{R^*E} > R_S | \mathcal{D} = \mathcal{D}_n\} = \Pr\{\gamma_{R^*E} > \Lambda_3\} = 1 - \Pr\{\gamma_{R^*E} < \Lambda_3\}$$

When $P_R/\sigma_E^2 \leq 2^{2R_S} P_J/\sigma_E^2$, we have $\Lambda_3 \leq 0$, and $\Pr\{C_{R^*E} > R_S | \mathcal{D} = \mathcal{D}_n\} = 1$.

Therefore, the closed-form expression for IP is:

$$P_{\text{int}} = \sum_{n=1}^{N} \binom{N}{n} \Phi_1^{N-n} (1-\Phi_1)^n (1-\Phi_3)$$

where $\Phi_3 = \Pr\{\gamma_{R^*E} < \Lambda_3\}$. From equation (19), when $\Lambda_3 > 0$, the closed-form expression for Φ_3 is:

$$\Phi_3 = \frac{1}{\Gamma(m_{R^*E})} \sum_{i=0}^{\infty} \frac{(-1)^i \lambda_{R^*E}^{m_{R^*E}+i} \Lambda_3^{m_{R^*E}+i}}{i!(m_{R^*E}+i)}$$

When $\Lambda_3 \leq 0$, $\Phi_3 = 0$.

2.3 Reliability-Security Tradeoff Analysis

For any communication system, both high reliability and high security are desired, which corresponds to both probabilities defined in equations (9) and (15) being as small as possible. However, existing research shows that these two performance metrics are actually contradictory and cannot both be minimized simultaneously. To comprehensively analyze system performance, this paper defines a tradeoff performance metric that includes both OP and IP [10]:

$$\mathcal{T} = (1 - P_{\text{out}}) \times (1 - P_{\text{int}})$$

Substituting the closed-form expressions for OP and IP derived above (equations (14) and (21)) into this equation yields the tradeoff performance of the proposed scheme:

$$\mathcal{T} = \left[1 - \Phi_1^N - \sum_{n=1}^{N} \binom{N}{n} \Phi_1^{N-n} (1-\Phi_1)^n \Phi_2\right] \times \left[1 - \sum_{n=1}^{N} \binom{N}{n} \Phi_1^{N-n} (1-\Phi_1)^n (1-\Phi_3)\right]$$

This expression shows that a larger $\mathcal{T}$ value indicates better system tradeoff performance, while a smaller $\mathcal{T}$ value indicates poorer tradeoff performance. Through this equation, the impact of various parameters on system performance can be conveniently obtained.

2.4 Power Allocation

To further improve the system' s tradeoff performance, consideration of power allocation in the system is necessary. The discussion proceeds for two cases: limited total system power and unlimited total system power.

When the total system power is limited, without loss of generality, assume the total system power is P_{tot}. Let the source transmit power be $P_S = \nu P_{\text{tot}}$, the

relay forwarding power be $P_R = \mu P_{\text{tot}}$, and the artificial interference transmit power be $P_J = (1-\mu-\nu)P_{\text{tot}}$, where μ and ν are power allocation factors. Therefore, the optimization problem can be expressed as:

$$\max_{\mu,\nu} \mathcal{T}(\mu,\nu)$$

$$\text{s.t. } 0 \le \mu \le 1, \quad 0 \le \nu \le 1, \quad \mu + \nu < 1$$

When the total system power is limited, the forwarding power and interference transmit power allocated to each relay are P_R/n and P_J/n, respectively (where n is the number of relays that can correctly decode in the first phase). As the number of relays increases, the forwarding power and artificial interference transmit power allocated to each relay continuously decrease, resulting in progressively worse system SRT performance.

When the total system power is unlimited, fixed power values are allocated to each relay. Theoretically, system performance continuously improves as the number of relays increases, but the total system power also increases correspondingly. Subsequent simulations will compare these two scenarios.

3 Simulation Analysis

This section presents a series of simulation analyses based on MATLAB. Unless otherwise specified, the default parameter values are: the target transmission rate $R_S = 0.1$ bits/s/Hz, the Nakagami shape factor $m = 1$, and the noise variances $\sigma_{SR}^2 = \sigma_{RD}^2 = \sigma_{RE}^2 = 1$. The channel coefficients in the simulation are independent and identically distributed. First, the system performance under power-limited and power-unlimited conditions is compared. Next, the power allocation under power-limited conditions is discussed. Finally, the SRT performance under different Nakagami-m fading channels with various values of m is compared and analyzed.

3.1 Comparison of Power-Limited and Power-Unlimited Cases

[Figure 2: see original paper] shows the simulation of system SRT performance versus the number of correctly decodable relays n under both power-limited (PL) and power-unlimited (nPL) cases. The theoretical analysis results (solid lines) and Monte Carlo simulation results (dotted lines) in the figure almost completely overlap, verifying the correctness of the outage probability and intercept probability derivations. In the PL case, $P_{\text{tot}} = 1$ is set. In the nPL case, case 1 and case 2 represent scenarios where the relay node power (sum of forwarding power and artificial interference transmit power) takes the values allocated to each relay when the number of correctly decodable relays is 15 and 25, respectively, in the PL case, with fixed power per relay regardless of the actual number of relays.

The figure shows that in the PL case, system SRT performance $\mathcal{T}$ first increases and then decreases with the number of correctly decodable relays n, reaching

its maximum at $n = 12$. When the number of relays is small, appropriately increasing the number of relays can improve system diversity gain and thus enhance reliability. The subsequent decline occurs because as the number of relays increases, the power allocated to each relay continuously decreases, reducing the power available for information forwarding and artificial interference transmission, thereby degrading system SRT performance. In the nPL case, system SRT performance $\mathcal{T}$ continuously increases with the number of relays n, stabilizing when the number of relays reaches a certain point. This is because as n increases, system reliability gradually peaks, while further increases in n do not change the system' s security level, causing the SRT performance to stabilize. However, in practical systems, power is a critical resource that cannot increase indefinitely, and the total system power is typically constant. Therefore, subsequent simulation analyses are primarily based on the PL case.

3.2 Finding the Optimal Configuration

Based on the optimal number of relays $n = 12$ obtained from [Figure 2: see original paper] for the PL case, the three-dimensional plot of system SRT performance versus μ and ν is shown in [Figure 3: see original paper]. The figure demonstrates that for a fixed ν, there exists a corresponding μ that maximizes system SRT performance. For the target rate $R_S = 0.1$ bits/s/Hz assumed in this paper, the optimal SRT performance is achieved at $\mu = 0.19$ and $\nu = 0.62$. Therefore, in subsequent power allocation simulations, $\mu = 0.19$ and $\nu = 0.62$ are used.

3.3 Optimal Power Allocation

Using the previously obtained optimal number of correctly decodable relays $n = 12$ for the PL case and the optimal SNR $\zeta = 15.5$ dB, the three-dimensional simulation of system SRT performance versus μ and ν is shown in [Figure 4: see original paper]. The optimal power allocation factor obtained from the figure is $\mu = 0.19$ and $\nu = 0.95$, with optimal system SRT performance $\mathcal{T} = 0.142$. At this point, the source node power allocation factor is $\nu = 0.95$, which differs from the previous simulation assumption of $\nu = 0.62$ because the current number of correctly decodable relays is 12, which is relatively large and consumes more system power, leaving less power for the source node. The artificial interference power is $P_J = 0.19P_{\text{tot}}$, and after averaging among the 12 relays, each receives only $0.0158P_{\text{tot}}$, showing that not much power is needed for transmitting artificial interference to achieve secure information transmission.

3.4 Simulation of Tradeoff Performance under Different Channel Conditions

Using the previously obtained optimal parameters $\mu = 0.19$ and $\nu = 0.62$, the simulation of system SRT performance versus SNR ζ under different channel conditions is shown in [Figure 5: see original paper]. The figure demonstrates

that the system SRT performance can approach 1 under all three channel conditions, indicating that the system can achieve reliable and secure information transmission. As ζ continuously increases (i.e., channel conditions improve), the SNR ζ required to achieve optimal SRT performance decreases, meaning that less system power is needed to achieve better SRT performance.

4 Conclusion

This paper proposes a cooperative secure transmission scheme based on artificial interference for multi-relay cooperative communication systems. In this scheme, opportunistic relays transmit artificial interference signals while forwarding source information to disrupt eavesdroppers and reduce their ability to intercept source information. Under Nakagami-m fading channels, the system' s security performance is analyzed, closed-form expressions for outage probability and intercept probability are derived, and these two probabilities are considered as a whole to conduct tradeoff analysis and system optimization from the perspectives of information transmission reliability and security. Computer simulations verify the accuracy of the theoretical analysis and clarify the impact of the number of relays on system security performance. Additionally, through simulations of the impact of power allocation among various signals on system tradeoff performance, the optimal power allocation factor that maximizes system tradeoff performance is obtained.

Artificial interference plays a crucial role in improving system security; however, existing literature rarely studies specific interference cancellation schemes for legitimate receivers. Future work will leverage existing interference cancellation and signal separation methods to design different cancellation schemes for various artificial interference signals, enabling efficient and secure information transmission.

Appendix A

Derivation of Φ_1, Φ_2, and Φ_3:

From the probability density function of γ_{SR_k} in equation (3), we obtain:

$$\Phi_1 = \Pr\{\gamma_{SR_k} < \Lambda_1\} = \int_0^{\Lambda_1} \frac{\lambda_{SR_k}^{m_{SR_k}} \gamma^{m_{SR_k}-1}}{\Gamma(m_{SR_k})} e^{-\lambda_{SR_k}\gamma} d\gamma$$

Using Taylor series expansion and integration yields:

$$\Phi_1 = \frac{1}{\Gamma(m_{SR_k})} \sum_{i=0}^{\infty} \frac{(-1)^i \lambda_{SR_k}^{m_{SR_k}+i} \Lambda_1^{m_{SR_k}+i}}{i!(m_{SR_k}+i)}$$

Similarly, the closed-form expression for Φ_2 is:

$$\Phi_2 = \Pr\{\gamma_{R^*D} < \Lambda_2\} = \frac{1}{\Gamma(m_{R^*D})} \sum_{i=0}^{\infty} \frac{(-1)^i \lambda_{R^*D}^{m_{R^*D}+i} \Lambda_2^{m_{R^*D}+i}}{i!(m_{R^*D}+i)}$$

For Φ_3, from equation (19), when $\Lambda_3 > 0$, the closed-form expression is:

$$\Phi_3 = \Pr\{\gamma_{R^*E} < \Lambda_3\} = \frac{1}{\Gamma(m_{R^*E})} \sum_{i=0}^{\infty} \frac{(-1)^i \lambda_{R^*E}^{m_{R^*E}+i} \Lambda_3^{m_{R^*E}+i}}{i!(m_{R^*E}+i)}$$

When $\Lambda_3 \leq 0$, $\Phi_3 = 0$.

References

[1] Nosratinia T E, Hunter, Hedayat A. Cooperative communication in wireless networks [J]. IEEE Communications Magazine, 2004, 42 (10): 74-80.

[2] Xiong Ying, Tang Lun, Chen Qianbin. Research on cooperative ARQ for two-hop and two-relay system [J]. Application Research of Computer, 2010, 27 (1): 311-313.

[3] Kim Y G, Beaulieu N C. SEP of decode-and-forward cooperative systems with relay selection in Nakagami-m fading channels [J]. IEEE Trans on Vehicular Technology, 2015, 64 (5): 1882-1894.

[4] Zhang Qianqian, Gao Yuanyuan, Zang Guozhen, et al. Physical layer security for cooperative communication system with untrusted relay based on jamming signals [C]// Proc of International Conference on Wireless Communications & Signal Processing. Piscataway, NJ: IEEE Press, 2015.

[5] Tubail D, El-Absi M, Ikki S, et al. Artificial noise based physical layer security in interference alignment multipair two-way relaying networks [J]. IEEE Access, 2018, 6: 19073-19085.

[6] Zhou Xiangyun, McKay M R, Maham B, et al. Rethinking the secrecy outage formulation: a secure transmission design perspective [J]. IEEE Communications Letters, 2011, 15 (3): 302-304.

[7] Zou Yulong, Wang Xianbin, Shen Weiming, et al. Security versus reliability analysis of opportunistic relaying [J]. IEEE Trans on Vehicular Technology, 2014, 63 (6): 2653-2661.

[8] Heidarpour A R, Ardakani M, Tellambura C. Generalized relay selection for network-coded cooperation systems [J]. IEEE Communications Letters, 2017, 21 (12): 2742-2745.

[9] Lei Hongjiang, Zhang Huan, Ansari I S, et al. On secrecy outage of relay selection in underlay cognitive radio networks over nakagami-m fading channels

[J]. IEEE Trans on Cognitive Communications and Networking, 2017, 3 (4): 614-627.

[10] Peng Lei, Zang Guozhen, Zhou Qian, et al. Security performance analysis for cooperative communication system under Nakagami-m fading channel [C]// Proc of IEEE International Conference on Communication Technology. Piscataway, NJ: IEEE Press, 2017: 187-192.

Note: Figure translations are in progress. See original paper for figures.