Security-Oriented Round-Robin Relay Selection Scheme Postprint

Authors: Qin Xiaogang, Zou Yi, Huang Kaizhi

Date: 2018-05-20T00:00:00+00:00

Abstract

To address the eavesdropping problem in multi-relay round-robin relaying systems, a security-oriented round-robin relay selection scheme is proposed. First, an exhaustive optimal relay selection scheme is presented, and the theoretical value of the secrecy rate is derived. Subsequently, to reduce complexity, two suboptimal two-stage relay selection schemes are designed from the perspectives of reducing computational complexity and channel estimation overhead, respectively, which first narrow down the relay selection range before conducting the search. Simulation results demonstrate that the K-best main channel relay selection scheme can achieve optimal secrecy rate with lower complexity.

Full Text

Preamble

Secure-Oriented Relay Selection Schemes in Successive Relaying Systems

Qin Xiaogang, Zou Yi, Huang Kaizhi
(China National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China)

Abstract: To address the eavesdropping problem in multi-relay successive relaying systems, this paper proposes security-oriented relay selection schemes. First, an optimal relay selection (OPRS) scheme is developed through exhaustive search, and the theoretical secrecy rate is derived. To reduce complexity, two suboptimal two-stage relay selection schemes are then designed from the perspectives of reducing computational complexity and channel estimation overhead, respectively, by first narrowing down the relay selection range before performing the search. Simulation results demonstrate that the K-maximum main channel relay selection scheme can achieve optimal secrecy rate with relatively low complexity.

Key Words: successive relaying; physical-layer security; relay selection; secrecy rate

0 Introduction

Cooperative communication technology can significantly improve the spectral efficiency of wireless networks, but the half-duplex nature of some relay stations limits further enhancement of spectral efficiency. Half-duplex relay stations cannot transmit and receive signals simultaneously, requiring at least two independent time slots for one information transmission, which leads to spectral efficiency loss. Full-duplex relays demand complex hardware design, and their self-interference, if not properly managed, can severely degrade system performance, making them unsuitable for many scenarios.

To overcome the half-duplex limitation of relay nodes, researchers have proposed the concept of successive relaying (SR), which simulates a full-duplex node by coordinating multiple half-duplex relays to alternately forward signals, thereby achieving simultaneous signal reception and transmission at relays. Leveraging SR technology enables continuous communication between source and destination nodes, improving system spectral efficiency. During SR communication, simultaneous transmissions from the source node and one relay node interfere at another relay node, with the signal forwarded from the other relay termed inter-relay interference (IRI). Existing studies show that signal processing techniques can mitigate IRI effects and effectively enhance communication capacity.

However, SR technology introduces new security challenges. While multiple relay nodes expand the coverage of confidential signals, they also increase the risk of relay links being eavesdropped. On the other hand, multi-relay networks provide favorable spatial cooperative resources for secure communication. Physical-layer security transmission techniques based on wireless channel characteristics can exploit relay cooperation resources to construct advantageous communication conditions for legitimate links, making them a research hotspot in recent years. Relay selection technology utilizes a small number of nodes to achieve optimal or near-optimal security performance with relatively low complexity, yielding significant research advances. Specifically, reference [8] discusses optimal relay selection schemes for various transmission strategies and compares their intercept probability and achievable diversity gains. Reference [9] proposes three optimal relay-user combination selection criteria for multi-user scenarios to minimize secrecy outage probability. Reference [10] considers adapting strategies to eavesdroppers and proposes optimal relay selection schemes under different channel information conditions, deriving secrecy outage probabilities. References [11-13] incorporate artificial noise into relay selection, where other nodes transmit friendly jamming. Reference [11] first proposes selecting one relay and one friendly jammer in multi-relay networks to enhance security. Reference [12] extends this method to two-way relay networks and proves that

secrecy rate outperforms conventional two-way relay networks when relay nodes are randomly distributed. Reference [13] further generalizes this approach by selecting the best channel relay to forward information while using other nodes as friendly jammers. Additionally, references [14,15] consider node selfishness and introduce game-theoretic models for relay and jammer selection.

Multi-relay SR systems also face relay selection challenges. Reference [16] addresses untrusted relays in SR systems by combining IRI cancellation with relay selection, proposing a fast relay selection method to achieve lower secrecy outage probability. However, no existing research has proposed using relay selection techniques to address external eavesdropping in multi-relay SR systems.

To tackle this problem, this paper proposes security-oriented relay selection schemes for successive relaying systems, including an optimal relay selection (OPRS) scheme, a K-maximum main channel relay selection (K-MMRS) scheme, and a K-maximum IRI relay selection (K-MIRS) scheme. The OPRS scheme obtains optimal secrecy performance through one-dimensional search to maximize secrecy rate, and the theoretical system secrecy rate is derived. However, when the number of relays is large, the computational complexity and channel estimation overhead of OPRS become excessive. To reduce complexity, the K-MMRS and K-MIRS schemes are proposed as two-stage suboptimal relay selection schemes from the perspectives of maximizing main channel capacity and maximizing IRI, respectively. Both schemes first narrow the relay selection range before performing exhaustive search, where K-MIRS has the lowest computational complexity and K-MMRS has the lowest channel estimation overhead. Simulation results validate these schemes and demonstrate that K-MMRS can achieve optimal security performance with relatively low computational complexity and channel estimation overhead.

1 System Model

This paper studies a multi-relay network model shown in [Figure 1: see original paper], which includes a legitimate source node (Alice), a legitimate destination node (Bob), an eavesdropper (Eve), and a set of N relay nodes that are relatively close to each other. All relay nodes operate under the amplify-and-forward protocol. Except for Alice, which is equipped with N_a antennas, all other nodes in the network have a single antenna and operate in half-duplex mode. No direct link exists between Alice and Bob, so communication must be established through relay nodes.

Assume that before communication begins, Alice obtains channel state information (CSI) between all nodes through channel estimation and selects the i-th relay (R_i) to participate in communication based on certain relay selection criteria. This assumption aligns with reference [13] and its cited works. During communication, only the activated relay participates while all other relays remain silent. The SR communication process is illustrated in [Figure 2: see original paper]. Without loss of generality, in odd time slots, Alice transmits

confidential information to R_i while R_j forwards the signal received in the previous time slot. In even time slots, Alice transmits to R_j while R_i forwards the previous signal. When links between relays exist, simultaneous transmissions from Alice and any relay create superimposed signals at the other relay, forming IRI. The presence of IRI degrades channel quality at legitimate nodes and can result in zero system secrecy rate.

Without loss of generality, assume Alice transmits signal $s(k)$ to R_i while R_j forwards the previously received signal $s(k-1)$ to Bob. Let $W(k)$ and $x(k)$ denote the beamforming vector and data symbol at time slot k, respectively, with $E\{|s(k)|^2\} = 1$. The original received signals at the relay and Bob contain IRI and are expressed as:

$$y_{r_i}(k) = \sqrt{P_a} h_{a,i} W(k) s(k) + \sqrt{P_j} \alpha_j h_{j,i} s(k-1) + n_i(k) \tag{1}$$

$$y_b(k) = \sqrt{P_j} \alpha_j h_{j,b} s(k-1) + \sqrt{P_a} h_{a,b} W(k) s(k) + n_b(k) \tag{2}$$

where p and q represent the indices of relays transmitting signals in time slots p and q, respectively, and $v = 0$ indicates no relay participates in signal forwarding during the first time slot. Assume wireless channels are affected by additive white Gaussian noise (AWGN) and that the channel from antenna i to node j is a non-frequency-selective Rayleigh block-fading channel following a complex Gaussian distribution with zero mean and variance δ_{ij}^2. Therefore, the channel gain $g_{ij} = |h_{ij}|^2$ follows an exponential distribution. Let P_a denote Alice' s average power constraint, α_i and α_j denote the amplification coefficients under average power constraint P_r, and $n(k)$ represents the AWGN variable at time slot k.

The IRI cancellation scheme from reference [16] can achieve complete IRI elimination at Bob, while Eve cannot perform similar IRI cancellation due to channel differences, causing mutual interference between adjacent confidential signals and effectively improving SR system security. Additionally, Alice employs zero-forcing beamforming technology [7] to create a null at Eve. With IRI cancellation in the SR system shown in [Figure 2: see original paper], the received signals at the relay, Bob, and Eve can be expressed as:

$$y_{r_i}(k) = \sqrt{P_a} h_{a,i} W(k) s(k) + \sqrt{P_j} \alpha_j h_{j,i} s(k-1) + n_i(k) \tag{3}$$

$$y_b(k) = \sqrt{P_j} \alpha_j h_{j,b} s(k-1) + n_b(k) \tag{4}$$

$$y_e(k) = \sqrt{P_a} h_{a,e} W(k) s(k) + \sqrt{P_i} \alpha_i h_{i,e} s(k-1) + n_e(k) \tag{5}$$

For analysis convenience, assume signals from Alice and IRI are much stronger than noise, so noise effects are neglected. From equations (3)-(5), the signal-to-interference-plus-noise ratios (SINRs) for Bob' s and Eve' s links are:

$$\gamma_{b,B} = \frac{P_r \alpha_j^2 g_{j,b}}{P_a g_{a,b}} \tag{6}$$

$$\gamma_{e,E} = \frac{P_a g_{a,e}}{P_r \alpha_i^2 g_{i,e} + P_r \alpha_j^2 g_{j,e}} \tag{7}$$

Since Alice has multiple antennas, $\gamma_{a,i}$ represents N independent random variables following a $\chi^2(2N_a)$ distribution. The cumulative distribution function (CDF) of $\gamma_{a,i}$ is:

$$F_{\gamma_{a,i}}(x) = 1 - e^{-x/\lambda_{a,i}} \sum_{n=0}^{N_a - 1} \frac{(x/\lambda_{a,i})^n}{n!}$$

where $\lambda_{a,i} = P_a \delta_{a,i}^2$. Therefore, the CDF of $\gamma_{a,n} = \max\{\gamma_{a,i}\}$ is $F_{\gamma_{a,n}}(x) = [F_{\gamma_{a,i}}(x)]^N$.

The system' s secrecy rate is:

$$R_s = \frac{1}{2} \left[\log_2(1 + \gamma_{b,B}) - \log_2(1 + \gamma_{e,E}) \right]^+$$

Since the IRI cancellation scheme is adopted, the eavesdropper channel capacity is less than the main channel capacity, so $(\log_2(1 + \gamma_{b,B}) - \log_2(1 + \gamma_{e,E})) > 0$ holds. Therefore:

$$R_s \approx \frac{1}{2} \log_2 \frac{\gamma_{b,B}}{\gamma_{e,E}}$$

Similarly, let $\gamma_{i,j} = P_r \alpha_i^2 g_{i,j}$ where random variable $g_{i,j}$ follows an exponential distribution. The calculation process for $E\{\gamma_{i,j}\}$ is similar to that for $E\{\gamma_{a,i}\}$.

When N available relay nodes exist in the SR system, two relay nodes must be selected for alternating forwarding to assist communication between Alice and Bob. Based on the above modeling, the next section addresses how to perform relay selection to ensure communication security.

2 Relay Selection Schemes

Unlike conventional relay systems, relay selection in SR systems must consider the impact of channel conditions between selected relay pairs on system performance. This section focuses on system security, using secrecy rate as the performance metric. First, the OPRS scheme is obtained through exhaustive search, and the theoretical secrecy rate for large relay numbers is analyzed. To reduce selection complexity, three two-stage relay selection schemes are proposed

from different perspectives affecting secrecy rate, with comparative analysis of computational complexity and channel estimation overhead.

2.1 OPRS Scheme

Since the expression for R_s is too complex for direct optimal relay pair selection, the optimal relay combination (R_i, R_j) must be found by exhaustively searching all possible relay pairs, calculating their secrecy rates, and selecting according to:

$$(R_i^*, R_j^*) = \arg \max_{i,j \in \mathcal{N}, i \neq j} R_s(i,j)$$

To evaluate different relay selection criteria, define C_f as the computational complexity coefficient, where $C_f = 1$ indicates the algorithm must traverse all possible relay pairs. Define C_e as the CSI overhead coefficient, where $C_e = 1$ indicates the algorithm requires global channel state information. The OPRS scheme uses one-dimensional search to select the optimal relay combination, requiring calculation of all possible C_N^2 relay pair combinations, yielding $C_f^{\text{OPRS}} = C_N^2$. The time complexity is $O(N^2)$, which becomes unacceptable when N is large.

When implementing OPRS, CSI for all relay links, eavesdropping links, and inter-relay channels must be estimated, requiring $C_e^{\text{OPRS}} = 3N + \frac{N(N-1)}{2}$ CSI quantities. To reduce implementation complexity, the following subsections propose three fast relay selection schemes that first narrow down candidate relays using specific criteria before applying exhaustive search.

The theoretical secrecy rate for large N is derived next. With many available relays, the channel gain between the optimal relay and Alice is typically large, so $\gamma_{a,n} \gg \gamma_{i,j}$ can be assumed. From the analysis, maximizing R_s is equivalent to maximizing $\frac{\gamma_{b,B}}{\gamma_{e,E}}$. Taking the derivative and setting it to zero yields the optimal $\lambda_{r,r}$:

$$\lambda_{r,r}^* = \frac{E\{\gamma_{a,i}\}E\{\gamma_{b,j}\}}{E\{\gamma_{i,j}\}}$$

The system secrecy rate can then be approximated as:

$$R_s \approx \frac{1}{2}\log_2 \frac{E\{\gamma_{a,i}\} + \lambda_{r,r}}{E\{\gamma_{i,j}\} + \lambda_{r,r}} \cdot \frac{E\{\gamma_{b,j}\} + \lambda_{r,r}}{\lambda_{r,r}}$$

2.2 K-MMRS Scheme

System secrecy rate depends on both main channel capacity and eavesdropper channel capacity. The K-MMRS scheme ensures main channel capacity by first

selecting K relays with the largest main channel gains $\gamma_{a,i}$ and $\gamma_{b,i}$ to reduce candidate size, then performing one-dimensional search:

$$(R_i^*, R_j^*) = \arg \max_{i,j \in \mathcal{C}_K, i \neq j} R_s(i,j)$$

where $\mathcal{C}_K$ denotes the set of K relays with largest main channel gains. This two-stage approach first reduces candidates to K relays, requiring computation of C_K^2 combinations in the second stage, so $C_f^{\text{K-MMRS}} = C_K^2$. In the first stage, CSI for all Alice-to-relay and relay-to-Bob channels is needed, while the second stage requires CSI among the K selected relays and between these relays and Eve. The total CSI overhead is $C_e^{\text{K-MMRS}} = 2N + K(K-1) + 2K$.

2.3 K-MIRS Scheme

The key difference between SR and conventional half-duplex relay systems is IRI. In the considered SR system, IRI processing degrades the eavesdropper' s channel while improving Bob' s signal quality, making IRI a security-enhancing factor. The K-MIRS scheme maximizes IRI impact by first selecting K relay pairs with the largest IRI (maximum inter-relay channel gains), then choosing the pair with best secrecy performance:

$$(R_i^*, R_j^*) = \arg \max_{i,j \in \mathcal{D}_K, i \neq j} R_s(i,j)$$

where $\mathcal{D}_K$ denotes the set of K relay pairs with IRI closest to the optimal $\lambda_{r,r}$. Like K-MMRS, this is a two-stage scheme, but the first stage filters K relay pairs based on IRI, leaving C_K^2 combinations for the second stage, so $C_f^{\text{K-MIRS}} = C_K^2$. For CSI overhead, K-MIRS first requires all inter-relay channels, then in the second stage needs CSI between the K relay pairs and other nodes (Alice, Bob, Eve), requiring up to $C_e^{\text{K-MIRS}} = \frac{N(N-1)}{2} + 4K$ CSI estimations.

3 Simulation Analysis

To verify the theoretical secrecy rate and compare relay selection schemes, simulations were conducted in MATLAB with unified parameters: AWGN power $\sigma^2 = 1$, average channel gains from Alice-to-relay and relay-to-Bob set to 1, $N_a = 4$ antennas at Alice, transmit power $P_a = P_r = 30$ dBm, and 10^4 Monte Carlo runs.

[Figure 3: see original paper] compares theoretical secrecy rate with optimal average secrecy rate versus relay count N, assuming average inter-relay channel gain of 9. Results show that achievable secrecy rate increases with N, consistent with theoretical analysis. As N grows, $E\{\gamma_{a,n}\}$ and $E\{\gamma_{b,n}\}$ increase, making R_s a monotonically increasing function of N. While $E\{\gamma_{e,E}\}$ is not monotonic in N, the optimal $\lambda_{r,r}$ adjusts with changing $E\{\gamma_{a,i}\}$ and $E\{\gamma_{b,j}\}$, compensating for potential losses. Physically, more available relays increase the likelihood of larger

main channel capacities while IRI keeps eavesdropper capacity low, increasing theoretical secrecy rate. The OPRS average secrecy rate slightly exceeds the theoretical value due to approximations in deriving $E\{\gamma_{a,i}\}$ and $E\{\gamma_{b,j}\}$, but the error is small (maximum 3.03% when $N \leq 400$).

[Figure 4: see original paper] shows average secrecy rate versus N for different schemes with $K = 10$ and inter-relay gain of 9. OPRS achieves the maximum secrecy rate. K-MMRS performs second-best, nearly matching OPRS when N is small ($N < 50$), with a gradually increasing but acceptable gap as N grows. K-MIRS, with lowest complexity and overhead, performs worst in secrecy rate and shows no improvement with increasing N, confirming that larger IRI is not always better and an optimal value exists for each channel condition.

[Figure 5: see original paper] illustrates average secrecy rate versus K with $N = 200$ and inter-relay gain of 9. All schemes' secrecy rates increase with K, with larger K increasing complexity and overhead. The rate of improvement is steep for small K but saturates as K grows. K-MMRS approaches the optimal value at $K = 8$, with minimal additional gain beyond this point despite higher complexity. K-MIRS slows after $K = 10$ but remains far from OPRS, with over 2 bit/s/Hz gap at $K = 20$.

[Figure 6: see original paper] analyzes K-MMRS performance as N increases, showing the average K needed for optimal performance, complexity coefficient, and CSI overhead coefficient. As N grows, the required K increases roughly linearly, with $K = 10$ sufficient for near-optimal secrecy rate when $N = 400$. Both computational complexity and CSI overhead are significantly reduced compared to OPRS, with complexity coefficient below 1% and CSI overhead coefficient below 10%.

Table 1 compares the three schemes in secrecy rate, computational complexity, and CSI overhead. OPRS is always optimal in secrecy rate but has high complexity when N is large. K-MMRS is suboptimal but superior to K-MIRS for the same K, with moderate complexity. K-MIRS has the lowest complexity but worst secrecy rate. For CSI overhead with large N and K, the ranking from low to high is: K-MMRS < K-MIRS < OPRS. In summary, OPRS offers optimal security but high complexity; K-MMRS suits scenarios with fast channel variations; K-MIRS suits scenarios with limited node computational capability.

4 Conclusion

This paper proposes multiple security-oriented relay selection schemes for SR systems with multiple available relays. First, an IRI cancellation method improves Bob' s signal quality while degrading Eve' s channel, ensuring SR system security. Based on this model, the OPRS scheme selects optimal relay combinations through exhaustive search, with derived theoretical secrecy rate. To address OPRS complexity, two two-stage schemes are proposed. Analysis and simulation show OPRS matches theoretical secrecy rate, while K-MMRS

achieves near-optimal performance with significantly reduced complexity and overhead.

References

[8] Zou Y, Wang X, Shen W. Optimal relay selection for physical-layer security in cooperative wireless networks [J]. IEEE Journal on Selected Areas in Communications, 2013, 31(10): 2099-2111.

[9] Fan L, Lei X, Duong T Q, et al. Secure multiuser communications in multiple amplify-and-forward relay networks [J]. IEEE Trans on Communications, 2014, 62(9): 3299-3310.

[10] Yang L, Chen J, Jiang H, et al. Optimal relay selection for secure cooperative communications with an adaptive eavesdropper [J]. IEEE Trans on Wireless Communications, 2016, 16(1): 26-42.

[11] Krikidis I, Thompson J S, Mclaughlin S. Relay selection for secure cooperative networks with jamming [J]. International Journal of Computer Science & Mobile Computing, 2009, 8(10): 5003-5011.

[12] Chen J, Zhang R, Song L, et al. Joint Relay and Jammer Selection for Secure Two-Way Relay Networks [J]. IEEE Trans on Information Forensics & Security, 2012, 7(1): 310-320.

[13] Wang C, Wang H M, Xia X G. Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks [J]. IEEE Trans on Wireless Communications, 2015, 14(2): 589-605.

[14] Zhang N, Cheng N, Lu N, et al. Partner selection and incentive mechanism for physical layer security [J]. IEEE Trans on Wireless Communications, 2015, 14(8): 4265-4276.

[15] 洪颖, 黄开枝, 罗文宇, 等. 一种基于两次报价博弈机制的安全中继选择方法 [J]. 信息工程大学学报, 2014, 15(5): 551-556.

[16] Wang W, Teh K C, Li K H. Relay selection for secure successive AF relaying networks with untrusted nodes [J]. IEEE Trans on Information Forensics & Security, 2016, 11(11): 2466-2476.

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