Hybrid Cache Placement for Physical-Layer Security in Cooperative Networks

Fang Shi, Weiqiang Tan, Junjuan Xia, Dongqing Xie, Lisheng Fan, and Xin Liu

***Abstract*—Due to the broadcast nature of wireless transmission, traditional wireless two-hop relaying is vulnerable for eavesdroppers to overhear messages. In order to enhance the physical-layer security, this paper studies one cooperative network with caching relays to reduce the transmission links overheard by the eavesdropper. Relays are grouped into different clusters so that the secrecy outage probability of any cluster is better than the traditional two-hop transmission. Based on the secrecy outage probability of clusters and the groups of files, we propose a novel hybrid cache placement (HCP) which combines the traditional base station caching strategy, most popular content caching strategy (MPC) and largest content diversity (LCD) caching strategy to cache the popular contents. The performance analysis and optimal design results are provided on the two objective functions: the secrecy outage probability and average secrecy capacity. From these two objective functions, some interesting observations are reached: for the function of secrecy outage probability, we can always find an optimal value of most popular files to minimize the secrecy outage probability, and for the function of average secrecy capacity, we can also find an optimal value of most popular files to maximize the average secrecy capacity. The numerical and simulation results are finally demonstrated to verify the proposed studies.**

***Index Terms*—Relay clusters, hybrid cache placement (HCP), physical layer security, secrecy outage probability, average secrecy capacity.**

I. INTRODUCTION

The issues of security have taken on an increasingly important role in wireless communication networks. Traditionally, cryptographic technologies are used to secure the communications, and a cipher system for the information theoretic analysis of cryptography was first proposed by Shannon in [1]. In [2], a theoretic foundation for physical layer security framework is proposed. In this paper, Wyner introduced a wiretap channel model, showed that secure communication is feasible without cryptography technology as long as the eavesdropper's channel is worse than the legitimate user's channel. From Wyner's wiretap channel model, the authors extended to study the secrecy capacity over Gaussian channel in [3]. The average secrecy capacity and secrecy outage probability in Rayleigh fading channels have been studied in [4]. To enhance the secrecy performance of wireless communications, relay and jammer selection techniques have been used in [5]–[13]. Specifically, the relaying techniques for enhancing the physical layer security have been studied in [5] and [9]. In [10] and [11], the optimal relay selection schemes based on AF and DF have been presented to improve wireless security and prevent eavesdropping attacks. The idea that selecting jammer sends intentional interference to jam the eavesdroppers has been studied in [7] and [12]. In addition, the works about the secrecy performance analysis have been studied in [14]–[20]. Specifically, the secrecy performance of dual-hop amplify-and-forward multi-antenna relaying systems over Rayleigh fading channels has been well studied in [16]. The works of roundrobin scheduling, optimal user scheduling and suboptimal user scheduling schemes to protect the CUs-CBS transmissions against the eavesdropping attacks have been presented in [17]. In [20], the authors presented the work about the transmit antenna selection for physical layer security of a MIMO system. And the other work of MIMO has been studied in [21]. Moreover, the work of joint user and relay selection algorithm for cooperative non-orthogonal multiple access networks has been studied in [22].

Recently, with the rapid development of modern wireless devices, the vast majority of demands for wireless data rates becomes higher and higher. Caching is emerging as a vital tool for alleviating capacity crunch in modern wireless networks. In [23], the authors proposed to combine distributed caching of content in small cells and cooperative transmissions from nearby base stations (BSs) to achieve unprecedented content delivery speeds and reduce back-haul cost and delay. In [24], the authors proposed a cell with many caching helpers which are equipped with memory for caching files, and proved caching placement found by the proposed greedy algorithm is optimal. The results in [25] have shown that it is not always optimal to follow the standard policy "cache the most popular content, everywhere". The work of [26] proposed a hybrid caching scheme that was jointly optimized with the transmission schemes, to achieve a fine balance between the signal cooperation gain and the caching diversity gain.

Caching and the physical layer security plays an important research in wireless networks. However, most of the existing studies did not fully explore and exploit their potential advantages. The works about secure caching have been studied in [27] and [28], where the problem of secure caching in the presence of an external wiretapper for both centralized and decentralized cache placement was analyzed.

In this paper, we propose a novel method to improve physical layer security in cooperative wireless networks and consider the caching into wiretap channel model. Based on the introduced model, the relays are grouped into different

F. Shi, W. Tan, J. Xia, D. Xie, and L. Fan are with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China (e-mail: shifang@e.gzhu.edu.cn, wqtan@gzhu.edu.cn, xiajunjuan@gzhu.edu.cn, dqxie@gzhu.edu.cn, lsfan@gzhu.edu.cn).

X. Liu is with School of Information and Communication Engineering, Dalian University of TechnologyDalian 116024, China (e-mail:liuxinstar1984@dlut.edu.cn).

The corresponding author is Lisheng Fan.

relay clusters so that the secrecy outage probability of each cluster is lower than traditional two-hop transmission and the files are also divided into three groups, the different caching strategies are used to cache the files of different groups. For example, if the files belong to the first group, the content caching strategy (MPC) caching strategy is employed and the files are cached at all relays, and when the user requests the file m belongs to the first group, all relays directly transmit the file to user. According to the received signal-to-noise ratio (SNR) at the user, we study the system performance and examine the optimal cache placement for two objective functions: Minimizing the secrecy outage probability and maximizing the average secrecy capacity.

The novelties and main contributions of this paper can be summarized as follows:

- We design the considered system by jointly considering the signal transmission scheme and hybrid cache placement, in order to improve the physical-layer security of the multiple DF relaying networks.
- For the hybrid cache placement, the closed-form expressions for the secrecy outage probability and the average secrecy capacity are derived. In addition, by optimizing the number of most popular file, we minimize the secrecy outage probability and the average secrecy capacity of the proposed system.
- The results demonstrate that the hybrid cache placement can improve the physical layer security in cooperative networks. Moreover, the system performance can be improved by increasing the value of p_s, p_r, C_R and γ. But the system performance will deteriorate with larger N.

The rest of this paper is organized as follows. In Section II, we present the system model and study the hybrid cache placement. Section III analyze the system performance on the two objective functions: The secrecy outage probability and the average secrecy capacity. The optimal designs for secrecy outage probability and average secrecy capacity are presented in Section IV. The numerical and simulation results are provided in Section V and the conclusions are presented in Section VI.

Notations: We use $\bar{P}$ and $\bar{C}_S$ to represent the secrecy outage probability and the average secrecy capacity, respectively. We use P^{Ti} and C^{Ti} to denote the secrecy outage probability and the average secrecy capacity of i-th transmission, respectively. And the notations P_{Cl}^{T2} and C_{Cl}^{T2} denotes the secrecy outage probability and the average secrecy capacity of relay cluster C_l in the second transmission scheme, respectively.

II. System Model

We consider a cooperation network with a BS, a legitimate user (D), an eavesdropper (E), and a middle node set $S_{\text{relay}} = \{1,2, \ldots, K\}$ as shown in Fig. 1. Without loss of generality, all relays are ordered by distance $d_{R_k,D}$, where R_1 is the closest one to D. In this system model, we consider BS has no direct link with D, and the transmission is performed only via relays. For legitimate D, if the requested files are cached in relays, relays transfer the file directly to D. But if

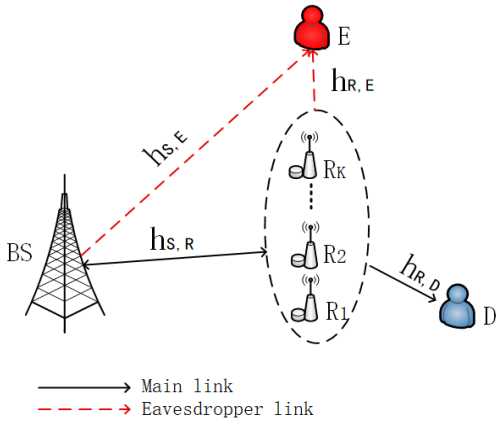


Fig. 1. An illustration of the cooperation network

the requested files are not cached in any relay, the traditional two-hop decode-and-forward protocol is employed. In the first phase, BS transmits its information to relay R_k among the middle node set S_{relay}, and because of the broadcasting nature of transmission, the eavesdropper also can overhear messages. In the second phase, we assume all relays can correctly decode the message from BS, and R_k decodes the message and forwards to D using the same codebook as S to R_k. We consider both phases over a Rayleigh flat fading channel and additive white Gaussian noise (AWGN) considered with zero mean and unit variance.

Herein, p_s and p_r represent the transmit power for BS and relay, respectively. $h_{i,j} = \sqrt{d_{i,j}^{-\alpha}}\widetilde{h}_{i,j}$ denotes the channel parameters of $i \to j$ and $\widetilde{h}_{i,j}$ is complex Gaussian random variable with zero mean and unit variance, where $d_{i,j}$ represents the distance between i and j, and $\alpha = 3$ is the path loss exponent.

A. Relay Clusters

As shown in the existing works such as [23] and [24], increasing number of relays in secure relaying networks can provide more signal cooperation diversity, and hence improve the secrecy performance significantly. Therefore, we can use relay clustering to exploit the signal cooperation diversity among relays, in order to enhance the transmission security. In our scheme, the cluster is adaptively formed by using a single threshold P^{T3}, which is the secrecy outage probability of the traditional two-hop transmission. There are some other clustering strategies, such as forming the clusters without using threshold, or forming the clusters by using multiple thresholds. For the clustering strategy without threshold, it does not need much prior information for clustering. However, the limitation of this strategy is that it cannot guarantee the secure performance. For the clustering strategy with multiple thresholds, it may provide better secrecy performance, at the cost of much more implementation complexity. Hence, by considering the trade-off between the performance and complexity, we adopt the clustering strategy with a single threshold P^{T3} in this paper.

In this paper, we consider P_{R_k} ($k \in [1, K]$) represents the

secrecy outage probability between R_k to D. According to P_{R_k} and P^{T3}, we can group relays to form L different relay clusters so that the secrecy outage probability of any cluster is lower than the traditional two-hop transmission. The details about the grouping of relays are shown as follows:

1) Calculate the secrecy outage probability of each relay and sort in ascending order according to secrecy outage probability of relay.
2) Find a threshold P_{R_k} ($k \in [1, K]$), it holds that $P_{R_k} < P^{T3}$, but $P_{R_{k+1}} > P^{T3}$. R_k divides relays into two different gathers $\{R_1, \ldots, R_k\}, \{R_{k+1}, \ldots, R_K\}$. In gather one $\{R_1, \ldots, R_k\}$, the secrecy outage probability of each relay is lower than P^{T3}, thus each relay form a cluster. In gather two $\{R_{k+1}, \ldots, R_K\}$, the secrecy outage probability of each relay is bigger than P^{T3}, we need to group relays belong to gather two to reform different clusters so that the secrecy outage probability of each cluster is lower than P^{T3}.
3) Add one relay from gather two in reverse order to a new cluster until cluster's secrecy outage probability is no greater than P^{T3} (R_K is the first one). But if all relays in gather two cannot reform a cluster that has lower probability than P^{T3}, they will be added to the last formed cluster in gather one.
4) After all clusters are formed, sort clusters in ascending order according to the secrecy outage probability of each cluster.

B. Hybrid Cache Placement

For traditional two-hop transmission, since the requested file is not cached at any relay, we consider this is a transmission without caching. In order to improve the rate of content delivery, cache has been applied to wireless networks. Such as MPC and LCD caching strategy which have been studied in [32]. In order to reduce the transmission links, we equip all relays with cache to store popular contents, and we combine MPC, LCD and relay without caching strategy to design a hybrid cache placement which can contribute to improve the physical security.

We assume that there are N files have been requested to D, which all have the same size and the unit of storage/size is file. The case of unequal size will not be considered in this paper, but we can always assume that any file can be divided into blocks of the same size, so the same analysis also can still be applied. In this paper, we consider files are characterized by their popularity, namely the probability that a file is requested by the user. And files are ordered according to their popularity f_n, $f_1 \geq f_2 \geq \ldots \geq f_N$, and $\sum_{n=1}^{N} f_n = 1$ $(1 \leq n \leq N)$. With Zipf distribution, the request probability of m-th popular file is given by

$$f_n = \frac{n^{-\gamma}}{\sum_{m=1}^{N} m^{-\gamma}}, \tag{1}$$

where γ is the Zipf parameter with the popularity skewness.

Since each relay has a limited storage capacity, we consider that storage capacity of each relay is C_R ($C_R \ll N$), and relays cannot store all files ($KC_R < N$), so each relay cluster needs to judiciously choose which files to store. In order to be more specific, we divide N files into three groups including most popular files, popular files and less popular files in terms of their popularity f_n:

- The first group: $G_1 = \{1, \ldots, M\}$, where M represents the number of most popular files. If the file belongs to the first group, it means the MPC caching strategy is employed and the file is cached in all relays.
- The second group: $G_2 = \{M+1, \ldots, Q(L, M)\}$, where L represents the number of relay clusters and $Q(l, M) \triangleq M + l(C_R - M)$. In Section II-A, all relays have been grouped into L different clusters $\{C_1, \ldots, C_L\}$. If the file belongs to the second group, the LCD caching strategy is employed and each cluster takes turn to store the next popular files, but those relays in the same cluster store the same files.
- The third group: $G_3 = \{Q(L, M)+1, \ldots, N\}$. The rest less popular files in the third group are not cached at any cluster, which means the requested file is cached at BS and must be forwarded from BS to D assisted by relay.

C. Transmission Schemes

In this subsection, we shall analyze the received SNRs at D and E of different transmission schemes according to the cache strategy of files. In addition, the transmit data rate is adaptively adjusted according to the instantaneous channel state. And in order to achieve the secrecy communication, the code can be designed as the random signals. In particular, the polar codes can be used to obtain the secure communications. The details about the secrecy codebook design can be found in [29] and [30].

In order to analyze the received SNRs at D and E, we use $\mathbf{h}_D = [h_{R_1,D}, h_{R_2,D}, \cdots, h_{R_K,D}]$ to denote the channel vector of the main links associated with K relays. Accordingly, the weighting vector at the relays $\mathbf{w}$ is equal to $\mathbf{h}_D^{\dagger}/||\mathbf{h}_D||_F$, where $(\cdot)^{\dagger}$ denotes conjugate transpose and $||\cdot||_F$ is the Frobenius norm.

1) Relay Clusters Collaborative Transmission: For relay cluster collaborative transmission, if the requested file m belongs to the first group, all clusters form collaborative beamforming to send it to D using the maximum ratio transmission principle. Hence, clusters directly transmit the cached file to the user when D sends the request, and the received SNR at D is given by

$$\mathsf{SNR}_{T1}^{\mathsf{D}} = \frac{p_r}{\sigma^2} \sum_{k=1}^{K} |h_{R_k,D}|^2, \tag{2}$$

where σ^2 is the noise power at the receiver. The received SNR at the eavesdropper E is given by

$$\mathsf{SNR}_{T1}^{\mathsf{E}} = \frac{p_r}{\sigma^2} \frac{\sum_{k=1}^{K} |h_{R_k,D}^{\dagger} h_{R_k,E}|^2}{\sum_{k=1}^{K} |h_{R_k,D}|^2}. \tag{3}$$

2) Relay Cluster Transmission: If the requested file m belongs to the second group, the corresponding relay cluster that stores it directly transmits it to D using maximum ratio transmission. When D sends the request, the file will be served

by a random relay cluster C_l, thus the received SNR at D served by cluster C_l is given by

$$\mathsf{SNR}^{\mathsf{D}}_{T2_{C_l}} = \frac{p_r}{\sigma^2}\sum_{k\in C_l}|h_{R_k,D}|^2. \tag{4}$$

The received SNR at E is given by

$$\mathsf{SNR}^{\mathsf{E}}_{T2_{C_l}} = \frac{p_r}{\sigma^2}\frac{\sum_{k\in C_l}|h^{\dagger}_{R_k,D}h_{R_k,E}|^2}{\sum_{k\in C_l}|h_{R_k,D}|^2} \tag{5}$$

3) Traditional Two-Hop Transmission: If the requested file m belongs to the third group, it means the traditional two-hop relaying is employed, and the best relay R_{k^*} is selected according to the standard max-min selection criterion, which maximizes the minimum of the dual-hop channel gains of main links. Thus, the received SNR at D is given by

$$\mathsf{SNR}^{\mathsf{D}}_{T3} = \min(\frac{p_s}{\sigma^2}|h_{S,R_{k^*}}|^2, \frac{p_r}{\sigma^2}|h_{R_{k^*},D}|^2). \tag{6}$$

The received SNR at E is given by

$$\mathsf{SNR}^{\mathsf{E}}_{T3} = \frac{p_s}{\sigma^2}|h_{S,E}|^2 + \frac{p_r}{\sigma^2}|h_{R_{k^*},E}|^2. \tag{7}$$

In this section, we have presented the system model and show transmission schemes for the hybrid cache placement. In the following section, we further analyze the system performance on the two objective functions: The secrecy outage probability and the average secrecy capacity.

III. PERFORMANCE ANALYSIS

In this section, we investigate the two key metrics for the system performance of proposed method, which includes the secrecy outage probability and average secrecy capacity. Moreover, we will derive the analytical results on secrecy outage probability and average secrecy capacity of different transmission schemes, respectively. In this paper, we consider the target secrecy rate is τ.

A. Secrecy Outage Probability

We assume that the N files have been requested to D, and three transmission schemes are used to transmit the files belong to different groups. Thus, if the set S_{relay} contains the requested files, we can obtain the secrecy outage probability of relay clusters collaborative transmission as [6]–[9]

$$P^{T1} = \Pr\left\{\left[\log_2(1+\mathsf{SNR}^{\mathsf{D}}_{T1}) - \log_2(1+\mathsf{SNR}^{\mathsf{E}}_{T1})\right] < \tau\right\}. \tag{8}$$

For relay cluster transmission, if the requested file is stored at a random relay cluster C_l, the secrecy outage probability for this file served by C_l is given by

$$P^{T2}_{C_l} = \Pr\left\{\left[\log_2(1+\mathsf{SNR}^{\mathsf{D}}_{T2_{C_l}}) - \log_2(1+\mathsf{SNR}^{\mathsf{E}}_{T2_{C_l}})\right] < \tau\right\}. \tag{9}$$

For traditional two-hop transmission, if the requested file belongs to the third group, it means the file is cached in BS, which must be forwarded from S to D assisted by relay. Thus, the secrecy outage probability is given by

$$P^{T3} = \Pr\left\{\left[\frac{1}{2}\log_2(1+\mathsf{SNR}^{\mathsf{D}}_{T3}) - \frac{1}{2}\log_2(1+\mathsf{SNR}^{\mathsf{E}}_{T3})\right] < \tau\right\}. \tag{10}$$

Herein, we further evaluate the system performance through the secrecy outage probability of proposed system. And from above analysis, we have obtained the analytical results on the secrecy outage probability of relay clusters collaborative transmission, relay cluster transmission and traditional two-hop transmission. Thus, according to the popularity of files, we can derive the secrecy outage probability of proposed system in following theorem.

Theorem 1: The secrecy outage probability is given by

$$\bar{P} = C_R^{1-\gamma}\varphi(\rho) + C_1, \tag{11}$$

where $\rho \triangleq M/C_R \in [0,1]$, C_1 is a constant and independent of the parameter ρ, and

$$\varphi(\rho) \triangleq (\rho^{1-\gamma}(P^{T1} - P^{T2}_{C_1}) + \sum_{l=1}^{L-1}(l-(l-1)\rho)^{1-\gamma}(P^{T2}_{C_l} - P^{T2}_{C_{l+1}}) + (L-(L-1)\rho)^{1-\gamma}(P^{T2}_{C_L} - P^{T3}))/(N^{1-\gamma}-1). \tag{12}$$

Proof: The proof is presented in Appendix A. ∎

Remark 1: From *Theorem* 1, we observe that the secrecy outage probability is a complicated function of M, and the value of M dynamically determines the secrecy outage probability and the numbers of files in different groups. However, because M is an integer variable, we introduce a new continuous variable $\rho \triangleq M/C_R$ to study the convexity of function.

Based on *Theorem* 1, we have an interesting observation summarized in the following corollary.

Corollary 1: For fixed the parameters ρ, C_R and L, $\bar{P}$ is a monotonically decreasing function with respect to γ.

Proof: According to *Theorem* 1, the first order partial derivative of $\bar{P}$ with respect to γ can be calculated as

$$\frac{\partial\bar{P}(\gamma)}{\partial\gamma} = C_R^{1-\gamma}\frac{\partial\varphi}{\partial\gamma} - C_R^{1-\gamma}\varphi(\rho)(\ln C_R). \tag{13}$$

where

$$\frac{\partial\varphi}{\partial\gamma} = \{\rho^{1-r}(P^{T1}-P^{T2}_{C_1})\left(N^{1-\gamma}\ln N-(N^{1-\gamma}-1)\ln\rho\right) + \sum_{l=1}^{L-1}(l-(l-1)\rho)^{1-\gamma}(P^{T2}_{C_l}-P^{T2}_{C_{l+1}})\left(N^{1-\gamma}\ln N-(N^{1-\gamma}-1)\ln(l-(l-1)\rho)\right) + (L-(L-1)\rho)^{1-\gamma}(P^{T2}_{C_L}-P^{T3})\left(N^{1-\gamma}\ln N-(N^{1-\gamma}-1)\ln(L-(L-1)\rho)\right)\}/(N^{1-\gamma}-1)^2, \tag{14}$$

Since $\partial\varphi/\partial\gamma < 0$ and $C_R^{1-\gamma}\varphi(\rho)\ln C_R > 0$, we can infer that $\partial\bar{P}(\gamma)/\partial\gamma < 0$, which implies that $\bar{P}$ is a monotonically decreasing function with respect to γ. ∎

From *Corollary* 1, we can draw useful insight on the impact of parameter γ. It is noted that increasing the value of γ

improves the secrecy outage probability for the reason that $\bar{P}$ is a monotonically decreasing function with respect to γ. And increasing the value of γ, the system performance ameliorates with larger γ.

B. Average Secrecy Capacity

In this subsection, the analytical results on the average secrecy capacity of several transmission schemes will be presented in the following. We consider that C^{T1} and C^{T3}, represent the average secrecy capacity of transmitting a file that belongs to the first group and the third group, respectively. For the file belongs to the second group, we consider that $C_{C_l}^{T2}$ represents the average secrecy capacity of transmitting a file served by cluster C_l.

If the requested file belongs to the first group, it means the relay clusters collaborative transmission scheme is employed to transmit the file. And we can obtain the secrecy outage probability of relay clusters collaborative transmission as [6]–[9]

$$C^{T1} = E\left\{\left[\log_2(1+\mathsf{SNR}_{T1}^{\mathsf{D}}) - \log_2(1+\mathsf{SNR}_{T1}^{\mathsf{E}})\right]^+\right\}, \tag{15}$$

where $[x]^+$ represents max(0,x).

For relay cluster transmission, if the file served by a random cluster C_l, the average secrecy capacity of transmitting a file is given by

$$C_{C_l}^{T2} = E\left\{\left[\log_2(1+\mathsf{SNR}_{T2_{C_l}}^{\mathsf{D}}) - \log_2(1+\mathsf{SNR}_{T2_{C_l}}^{\mathsf{E}})\right]^+\right\}. \tag{16}$$

For traditional two-hop transmission, if the file is transmitted from BS to D assisted by relay R_{k^*}, the average secrecy capacity for is given by

$$C^{T3} = E\left\{\left[\frac{1}{2}\log_2(1+\mathsf{SNR}_{T3}^{\mathsf{D}}) - \frac{1}{2}\log_2(1+\mathsf{SNR}_{T3}^{\mathsf{E}})\right]^+\right\}. \tag{17}$$

In this subsection, our purpose is to evaluate the system performance with the average secrecy capacity in following theorem.

Theorem 2: The average secrecy capacity is given by

$$\bar{C}_S = C_R^{1-\gamma}\phi(\rho) + C_2, \tag{18}$$

where C_2 is a constant (not a function of ρ) and

$$\phi(\rho) \triangleq (\rho^{1-\gamma}(C^{T1} - C_{C_1}^{T2}) + \sum_{l=1}^{L-1}(l-(l-1)\rho)^{1-\gamma}(C_{C_l}^{T2} - C_{C_{l+1}}^{T2}) + (L-(L-1)\rho)^{1-\gamma}(C_{C_L}^{T2} - C^{T3}))/(N^{1-\gamma}-1). \tag{19}$$

Proof: The proof is presented in Appendix B. ∎

Remark 2: From *Theorem* 2, some useful insights on the impact of ρ are drawing. It can be seen that the secrecy outage probability is a complicated function of ρ, whose value determines the value of secrecy outage probability.

Based on above analysis, an important corollary is presented in the following.

Corollary 2: Given the fixed parameters ρ, C_R and L, $\bar{C}_S$ is a monotonically increasing function with respect to γ.

Proof: According to *Theorem* 2, the first order partial derivative of $\bar{C}_S$ with respect to γ is calculated by

$$\frac{\partial \bar{C}_S(\gamma)}{\partial \gamma} = C_R^{1-\gamma}\frac{\partial \phi}{\partial_\gamma} - C_R^{1-\gamma}\phi(\rho)\ln C_R. \tag{20}$$

where

$$\frac{\partial \phi}{\partial \gamma} = \{\rho^{1-r}(C^{T1} - C_{C_1}^{T2})\left(N^{1-\gamma}\ln N - (N^{1-\gamma}-1)\ln\rho\right) + \sum_{l=1}^{L-1}(l-(l-1)\rho)^{1-\gamma}(C_{C_l}^{T2} - C_{C_{l+1}}^{T2})\left(N^{1-\gamma}\ln N - (N^{1-\gamma} -1)\ln(l-(l-1)\rho)\right) + (L-(L-1)\rho)^{1-\gamma}(C_{C_L}^{T2} - C^{T3})\left(N^{1-\gamma}\ln N - (N^{1-\gamma}-1)\ln(L-(L-1)\rho)\right)\}/(N^{1-\gamma}-1)^2, \tag{21}$$

As $\partial\phi/\partial\gamma > 0$ and $C_R^{1-\gamma}\phi(\rho)\ln C_R < 0$, we know that $\partial\bar{C}_S(\gamma)/\partial\gamma > 0$, which indicates that $\bar{C}_S$ is a monotonically increasing function with respect to γ. ∎

From (20), it is obvious that the value of parameter γ effects the secrecy outage probability. And in terms of *Corollary* 2, we know that $\bar{C}_S$ is a monotonically increasing function with respect to γ, which shows that increasing the value of γ can improve the average secrecy capacity and the system performance.

IV. Optimization of Hybrid Cache Placement

From the performance analysis, it can be seen that the parameter M determines the cache placement and system performance. Therefore, the optimization of hybrid cache placement is to identify the optimal value of M. But since M is an integer variable, we firstly identify the optimal value of ρ, and then find the optimal M^* in terms of $M^* = \lceil \rho^* C_R \rceil$.

In order to obtain the optimal cache space assignment, we define two optimization problems in this section, including optimal design for secrecy outage probability and optimal design for average secrecy capacity.

A. Optimal Design for Secrecy Outage Probability

In this subsection, the optimal caching design is to identify the optimal value M^* to minimize the secrecy outage probability. From (11) and (12), we observe that both $\bar{P}$ and $\varphi(\rho)$ are polynomial functions of ρ. And according to the convexity of $\bar{P}$ and $\varphi(\rho)$, the approximately optimal cache placement strategy about secrecy outage probability is shown as follow.

Theorem 3: When the secrecy outage probability of clusters are the same, i.e., $P^{T2} = P_{C_l}^{T2}, l = 1, \ldots, L$, and the file requested from the second group is served by a random relay cluster. The approximately optimal cache placement strategy is given by

$$M^* = \lceil \rho^* C_R \rceil, \tag{22}$$

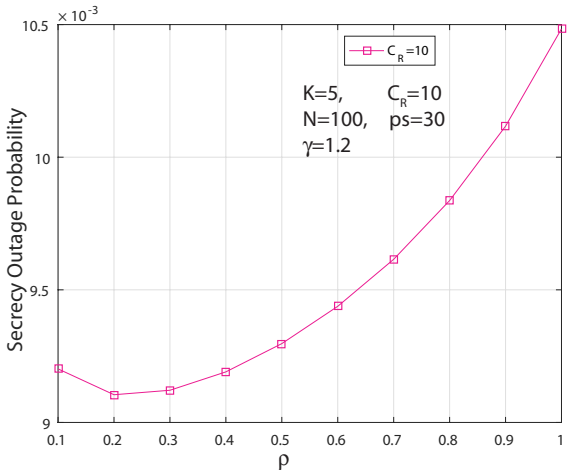


Fig. 2. Effect of ρ on function of secrecy outage probability.

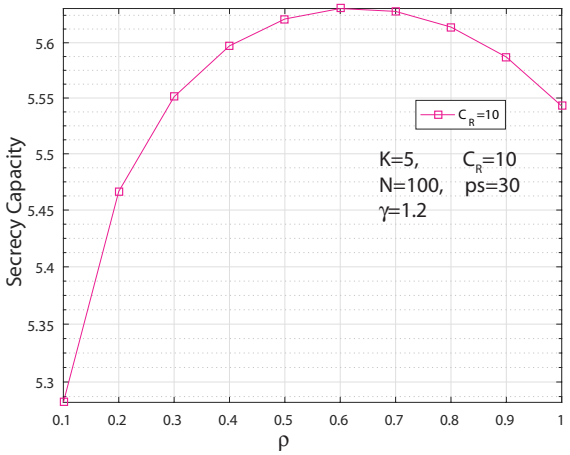


Fig. 3. Effect of ρ on function of average secrecy capacity.

where

$$\rho^* = \min(\rho^\dagger, 1), \tag{23}$$

with

$$\rho^\dagger \triangleq \frac{L}{\left(\frac{P^{T2}-P^{T1}}{(P^{T3}-P^{T2})(L-1)}\right)^{-1/\gamma} + (L-1)}. \tag{24}$$

Proof: The proof is presented in Appendix C. ■

Remark 3: According to the result of *Theorem* 3 and the proof in Appendix C, we know that both of the functions $\varphi(\rho)$ and $\bar{P}$ are convex functions with respect to ρ. So we can use bisection search to find the optimal ρ^*. And from (24), we can make an intuitive analysis on the impact of system parameters. It is noted that ρ^* depends on the ratio of $\frac{P^{T2}_{C_1}-P^{T1}}{P^{T3}-P^{T2}_{C_1}}$. Additionally, when $\frac{P^{T2}_{C_1}-P^{T1}}{P^{T3}-P^{T2}_{C_1}} < L-1$ and $\rho^\dagger < 1$, $\rho^\dagger$ is increasing with γ, and $\rho^* = \rho^\dagger$ is optimal in this case. When $\frac{P^{T2}_{C_1}-P^{T1}}{P^{T3}-P^{T2}_{C_1}} > L-1$ and $\rho^\dagger > 1$, $\rho^* = 1$. It means to store the most popular content is optimal.

The effect of ρ on secrecy outage probability is shown in Fig. 2. In our simulation, we set $K = 5, C_R = 10, \gamma = 1.2, p_s = 30$ dB, and $N = 100$. From the figure, we can find that the variable ρ determines the secrecy outage probability of proposed system and the secrecy outage probability is a convex function with respect to ρ. In addition, the minimum of secrecy outage probability is obtained at $\rho^* = 0.2$. This happens when the three caching strategies are all employed, and the optimal design for secrecy outage probability is $M^* = 2$.

B. Optimal Design for Average Secrecy Capacity

Different with optimal design for secrecy outage probability, our optimal caching design in this subsection is to identify the optimal value M^* to maximize the average secrecy capacity.

From (18), it can be seen that the parameter ρ determines the average secrecy capacity of proposed system. In order to maximize the average secrecy capacity, we present the following corollary and the approximately optimal cache placement strategy about average secrecy capacity is shown as follows.

Theorem 4: When the average secrecy capacity of relay clusters are identical, i.e., $C^{T2} = C^{T2}_{C_l}, l = 1, \ldots, L$, the file requested from the second group is served by a random relay cluster, the approximately optimal cache placement strategy is given by

$$M^* = \lceil \rho^* C_R \rceil, \tag{25}$$

where

$$\rho^* = \min(\rho^\ddagger, 1), \tag{26}$$

with

$$\rho^\ddagger \triangleq \frac{L}{\left(\frac{C^{T2}-C^{T1}}{(C^{T3}-C^{T2})(L-1)}\right)^{-1/\gamma} + (L-1)}. \tag{27}$$

Proof: The proof is presented in Appendix D. ■

Remark 4: Similarly to the analysis in optimal design for secrecy outage probability, from (27), it can be observed that ρ^* depends on the ratio of $\frac{C^{T2}_{C_1}-C^{T1}}{C^{T3}-C^{T2}_{C_1}}$, and when $\frac{C^{T2}_{C_1}-C^{T1}}{C^{T3}-C^{T2}_{C_1}} < L-1$ and $\rho^\ddagger < 1$, $\rho^* = \rho^\ddagger$. It means the hybrid cache placement strategy is employed in this case. When $\frac{C^{T2}_{C_1}-C^{T1}}{C^{T3}-C^{T2}_{C_1}} > L-1$ and $\rho^\ddagger > 1$, $\rho^* = 1$. It means MPC caching strategy is optimal in this case.

The effect of ρ on average secrecy capacity is shown in Fig. 3. In our simulation, we set $K = 5, C_R = 10, \gamma = 1.2, p_s = 30$ dB, and $N = 100$. It is obvious that the average secrecy capacity is a concave function with respect to ρ and when $\rho = 0.6$ the average secrecy capacity of proposed system have the maximum. It means that the hybrid cache placement is optimal in this case, and the optimal design for secrecy outage probability is $M^* = 6$. Comparing to the optimal design for secrecy outage probability, we can find that even if the conditions and the methods of optimal design are same, the result of optimal design is different.

V. NUMERICAL AND SIMULATION RESULTS

In this section, the numerical and simulation results are presented to verify the performance of system with hybrid cache placement proposed in this paper, and illustrate the effect of key system parameters. In addition, the system

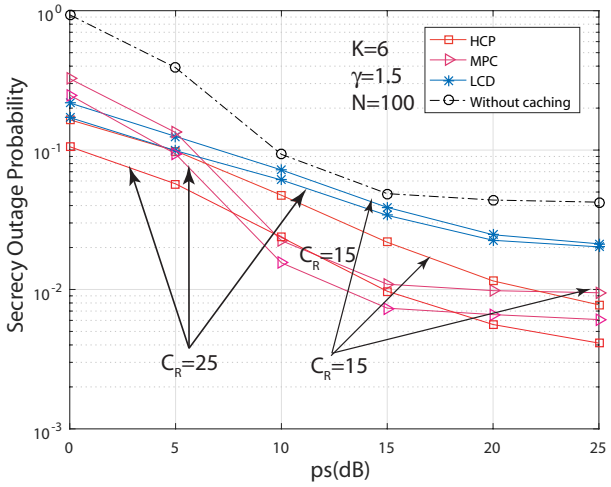


Fig. 4. Effect of p_s and C_R on secrecy outage probability.

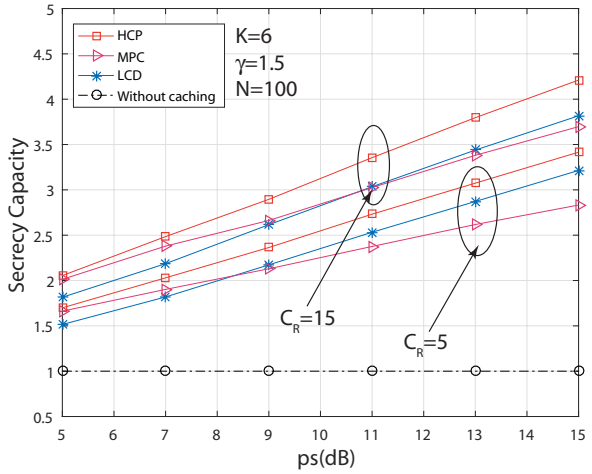


Fig. 5. Effect of p_s and C_R on average secrecy capacity.

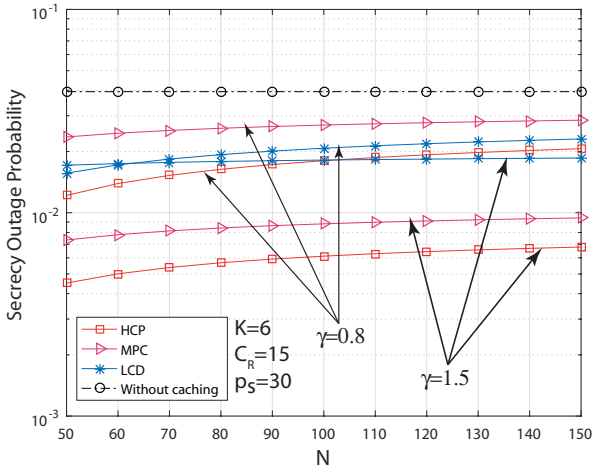


Fig. 6. Effect of N and γ on secrecy outage probability.

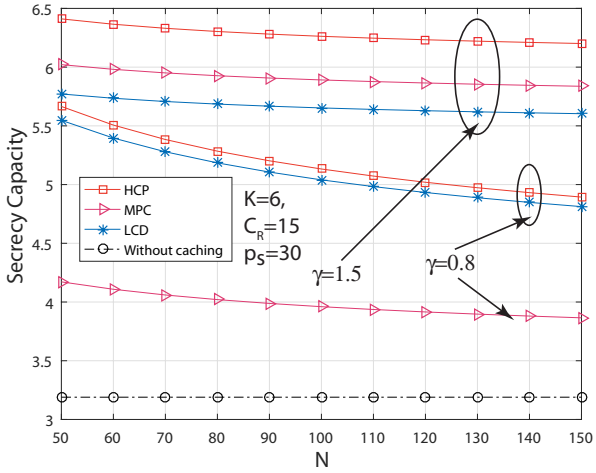


Fig. 7. Effect of N and γ on secrecy capacity.

performances are compared with MPC, LCD and relay without caching. In this paper, we consider there are K relays with cache capacity, $d_{S,R_k} = (K-k+1)/2, d_{R_k,D} = k/2$. The target secrecy rate τ is equal to 0.2 bps/Hz, the transmit power of relay $p_r = p_s/5$ and the noise power is set to one.

Fig. 4 shows the effect of transmit power and C_R on secrecy outage probability. In our simulations, we set $K = 6, \gamma = 1.5, N = 100, d_{S,E} = K$ and $d_{R_k,E} = 4\ d_{R_k,D}$. As observed from the picture, we can find that the value of C_R dynamically determines the system secrecy outage probability, and the secrecy outage probability of $C_R = 25$ is lower than $C_R = 5$, which illustrates that the secrecy outage probability ameliorates with larger C_R. And it is also obvious the secrecy outage probability ameliorates with larger N.

Fig. 5 shows the effect of transmit power and C_R on system average secrecy capacity. In our simulations, we set $K = 6, \gamma = 1.5, N = 100, d_{S,E} = K$ and $d_{R_k,E} = 4\ d_{R_k,D}$. As shown in picture, the average secrecy capacity of system with hybrid cache placement is higher than relay without caching strategy, MPC and LCD, which demonstrates our opinions that the hybrid cache placement can effectively improve the physical layer security. It is also obvious that the average secrecy capacity improves with larger transmit power, and the average secrecy capacity increase with the value of C_R.

Fig. 6 depicts the effect of key system parameters N and γ on system average secrecy outage probability, where $K = 6, C_R = 15$ and $p_s = 30$ dB. From the picture, we can see that the secrecy outage probability of hybrid cache placement is lower than relay without caching strategy, MPC and LCD. In addition, comparing the secrecy outage probability of $\gamma = 0.8$ and $\gamma = 1.5$, it is obvious that the secrecy outage probability ameliorates with larger γ and deteriorates with larger N.

In Fig. 7, we depict the effect of key system parameters N and γ on system average secrecy capacity. In our simulations, we set $K = 6, C_R = 15$, and $p_s = 30$ dB. As observed from the figure, the average secrecy capacity of system with hybrid cache placement is higher than relay without caching strategy, MPC and LCD, which supports our opinions that utilizing hybrid cache placement can effectively improve the physical layer security in cooperative networks. In addition, comparing the average secrecy capacity of $\gamma = 0.8$ and $\gamma = 1.5$, it is obvious that the average secrecy capacity ameliorates

with larger γ and deteriorates with larger N.

VI. CONCLUSIONS

In this paper, we proposed a novel method that using the hybrid cache placement to improve the physical layer security in cooperative networks. The main idea of hybrid cache placement is combining three different cache strategies to cache different files in terms of the secrecy outage probability of relay clusters and the popularity of files. We presented the performance analysis results and optimal design results on secrecy outage probability and average secrecy capacity, and some interesting observations are reached. For secrecy outage probability, we know that there always exists an optimal value of most popular files to minimize the secrecy outage probability, and for average secrecy capacity, we also see that there always exists an optimal value of most popular files to maximize the average secrecy capacity. Finally, the numerical simulations were provided to verify our analytical results that utilizing hybrid cache placement can contribute to improve the physical layer security in cooperative networks.

ACKNOWLEDGEMENTS

This work was supported by the NSF of China (No. 61372129), by the Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2014A030306027), by the Innovation Team Project of Guangdong Province University (No. 2016KCXTD017), and by the Graduate Innovative Research Grant Program of Guangzhou University (No. 2017GDJC-M17).

APPENDICES

A. Proof of Theorem 1

According to the popularity of files, the secrecy outage probability can be shown as follow,

$$\bar{P} = P^{T1}\sum_{n=1}^{M} f_n + \sum_{l=1}^{L} P_{C_l}^{T2} \sum_{n=Q(l,M)+M-C+1}^{Q(l,M)} f_n + P^{T3}\left(1 - \sum_{n=1}^{Q(L,M)} f_n\right). \tag{28}$$

By invoking the expression $Q(l,M) \triangleq M + l(C_R - M)$, the secrecy outage probability can be extended as

$$\bar{P} = P^{T1}\sum_{n=1}^{M} f_n + \sum_{l=1}^{L} P_{C_l}^{T2}\left(\sum_{n=1}^{l(C_R-M)+M} f_n - \sum_{n=1}^{l(C_R-M)+2M-C_R} f_n\right) + P^{T3}\left(1 - \sum_{n=1}^{L(C_R-M)+M} f_n\right). \tag{29}$$

In order to minimize the secrecy outage probability, we invoke the following result of approximating the sum of Zipf probabilities [33]

$$\sum_{n=1}^{m} f_n \approx \frac{m^{1-\gamma}-1}{N^{1-\gamma}-1}. \tag{30}$$

Based on the above approximation, the secrecy outage probability of system with hybrid cache placement can be shown as

$$\bar{P} = P^{T1}\frac{M^{1-\gamma}-1}{N^{1-\gamma}-1} + \sum_{l=1}^{L} P_{C_l}^{T2}\left(\frac{(l(C_R-M)+M)^{1-\gamma}-1}{N^{1-\gamma}-1} - \frac{(l(C_R-M)+2M-C_R)^{1-\gamma}-1}{N^{1-\gamma}-1}\right) + P^{T3}\left(1 - \frac{(L(C_R-M)+M)^{1-\gamma}-1}{N^{1-\gamma}-1}\right). \tag{31}$$

Invoking the continuous variable ρ, the secrecy outage probability can be simplified as

$$\bar{P} = \frac{C_R^{1-\gamma}}{N^{1-\gamma}-1}(\rho^{1-\gamma}(P^{T1} - P_{C_1}^{T2}) + \sum_{l=1}^{L-1}(l-(l-1)\rho)^{1-\gamma}(P_{C_l}^{T2} - P_{C_{l+1}}^{T2}) \tag{32}$$

$$+ (L-(L-1)\rho)^{1-\gamma}(P_{C_L}^{T2} - P^{T3})) - \frac{P^{T1}-P^{T3}}{N^{1-\gamma}-1} + P^{T3} = C_R^{1-\gamma}\varphi(\rho) + C_1 \tag{33}$$

B. Proof of Theorem 2

Similarly, according to the popularity of files, the average secrecy capacity is given by

$$\bar{C}_S = C^{T1}\sum_{n=1}^{M} f_n + \sum_{l=1}^{L} C_{C_l}^{T2} \sum_{n=Q(l,M)+M-C+1}^{Q(l,M)} f_n + C^{T3}\left(1 - \sum_{n=1}^{Q(L,M)} f_n\right). \tag{34}$$

Invoking the expression $Q(l,M) \triangleq M + l(C_R - M)$ and approximating the sum of Zipf probabilities, the average secrecy capacity can be shown as

$$\bar{C}_S = \frac{C_R^{1-\gamma}}{N^{1-\gamma}-1}\left(\left(\frac{M}{C_R}\right)^{1-\gamma}(C^{T1} - C_{C_1}^{T2}) + \sum_{l=1}^{L-1}\left(l-(l-1)\frac{M}{C_R}\right)^{1-\gamma}(C_{C_l}^{T2} - C_{C_{l+1}}^{T2}) + \left(L-(L-1)\frac{M}{C_R}\right)^{1-\gamma}(C_{C_L}^{T2} - C^{T3}) - \frac{1}{C_R^{1-\gamma}}(C^{T1} - C^{T3})\right) + C^{T3}. \tag{35}$$

Since M is an integer variable, similarly, we introduce the

continuous variable ρ, $\bar{C}_S$ also can be shown as

$$\begin{aligned}\bar{C}_S = &\frac{C_R^{1-\gamma}}{N^{1-\gamma}-1}(\rho^{1-\gamma}(C^{T1}-C_{C_1}^{T2}) \\ &+\sum_{l=1}^{L-1}(l-(l-1)\rho)^{1-\gamma}(C_{C_l}^{T2}-C_{C_{l+1}}^{T2}) \qquad (36)\\ &+(L-(L-1)\rho)^{1-\gamma}(C_{C_L}^{T2}-C^{T3}))-\frac{C^{T1}-C^{T3}}{N^{1-\gamma}-1}+C^{T3} \\ =&C_R^{1-\gamma}\phi(\rho)+C_2, \qquad (37)\end{aligned}$$

C. Proof of Theorem 3

By differentiating $\varphi(\rho)$ with respect to ρ, the first order partial derivative of $\varphi(\rho)$ can be calculated as

$$\begin{aligned}\frac{\varphi'(\rho)}{\frac{1-\gamma}{N^{1-\gamma}-1}} = &\rho^{-\gamma}(P^{T1}-P_{C_1}^{T2}) \\ &+\sum_{l=1}^{L-1}(l-(l-1)\rho)^{-\gamma}(l-1)(P_{C_l}^{T2}-P_{C_{l+1}}^{T2}) \\ &+(L-(L-1)\rho)^{-\gamma}(L-1)(P_{C_L}^{T2}-P^{T3}). \qquad (38)\end{aligned}$$

Since the value of the first order partial derivative is not sure, it is necessary to further check the second order partial derivative of $\varphi(\rho)$, which can be expressed as

$$\begin{aligned}\frac{\varphi''(\rho)}{\frac{\gamma(\gamma-1)}{N^{1-\gamma}-1}} = &\rho^{-\gamma-1}(P^{T1}-P_{C_1}^{T2}) \\ &+\sum_{l=1}^{L-1}(l-(l-1)\rho)^{-\gamma-1}(l-1)^2(P_{C_l}^{T2}-P_{C_{l+1}}^{T2}) \\ &+(L-(L-1)\rho)^{-\gamma-1}(L-1)^2(P_{C_L}^{T2}-p^{T3}). \qquad (39)\end{aligned}$$

Based on caching model, we know that $P^{T1} < P_{C_1}^{T2}$, $P_{C_l}^{T2} < P_{C_{l+1}}^{T2}$, $P_{C_L}^{T2} < P^{T3}$, and $\frac{\gamma(\gamma-1)}{N^{1-\gamma}-1} < 0$. Therefore, we know $\varphi''(\rho) > 0$, it indicates that $\varphi(\rho)$ is a convex function with respect to ρ. And since $\bar{P} = C_R^{1-\gamma}\varphi(\rho)+C_1$, $\bar{P}$ is also a convex function with respect to ρ.

Since $\bar{P}$ is a convex function with respect to ρ, it shows that the optimal ρ^* is the critical point $\rho^\dagger$ that corresponds to zero first-order derivative.

D. Proof of Theorem 4

Similarly, by differentiating the $\phi(\rho)$ with respect to ρ, the first order partial derivative of $\phi(\rho)$ can be calculated as

$$\begin{aligned}\frac{\phi'(\rho)}{\frac{1-\gamma}{N^{1-\gamma}-1}} = &\rho^{-\gamma}(C^{T1}-C_{C_1}^{T2}) \\ &+\sum_{l=1}^{L-1}(l-(l-1)\rho)^{-\gamma}(l-1)(C_{C_l}^{T2}-C_{C_{l+1}}^{T2}) \\ &+(L-(L-1)\rho)^{-\gamma}(L-1)(C_{C_L}^{T2}-C^{T3}). \qquad (40)\end{aligned}$$

Because it is challenging to work out whether (40) is strictly positive or negative, the second order partial derivative of $\phi(\rho)$ is further checked, which gives

$$\begin{aligned}\frac{\phi''(\rho)}{\frac{\gamma(\gamma-1)}{N^{1-\gamma}-1}} = &\rho^{-\gamma-1}(C^{T1}-C_{C_1}^{T2}) \\ &+\sum_{l=1}^{L-1}(l-(l-1)\rho)^{-\gamma-1}(l-1)^2(C_{C_l}^{T2}-C_{C_{l+1}}^{T2}) \\ &+(L-(L-1)\rho)^{-\gamma-1}(L-1)^2(C_{C_L}^{T2}-C^{T3}). \qquad (41)\end{aligned}$$

Since $C^{T1} > C_{C_l}^{T2}, C_{C_l}^{T2} > C_{C_{l+1}}^{T2}, C_{C_L}^{T2} > C^{T3}$, and $\frac{\gamma(\gamma-1)}{N^{1-\gamma}-1} < 0$. Therefore, we have $\phi''(\rho) < 0$, it indicates that $\phi''(\rho)$ is a concave function with respect to ρ. And since $\bar{C}_S = C_R^{1-\gamma}\phi(\rho)+C_2$, $\bar{C}_S$ is also a concave function with respect to ρ.

Since $\bar{C}_S$ is a concave function with respect to ρ, the optimal ρ^* is the critical point ρ^* that corresponds to zero first-order derivative.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Jun. 1949.

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

[3] S. Leung-Yan-cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory,* vol. 24, no. 4, pp. 451-456, May 1978.

[4] M. Bloch, J. Barros, M. Rodrigues, and R. D. Mclaughlin "Wireless information-theoretic security", *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[5] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494-1505, Dec. 2016.

[6] L. Fan, R. Zhao, F. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811-2820, July 2017.

[7] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Commun.*, vol. 64, no. 24, pp. 6391-6401, Oct. 2014.

[8] A. Nahari, K. Ioannis, A. S. Ibrahim, and M. I. Dessouky, "Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers", *European Trans. Telecommunications*, vol. 25, no. 4, pp. 445-460, Apr. 2014.

[9] F. A. Qahtani, C. Zhong, and H. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756-1770, May 2015.

[10] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[11] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy Cooperative Networks With Outdated Relay Selection Over Correlated Fading Channels," *IEEE Trans. Vehicular Technology*, vol. 66, no. 8, pp. 7599-7603, Aug. 2017.

[12] F. Saeidikhabisi, V. Vakili, and D. Abbasimoghadam, "Improving the physical layer security in cooperative networks with multiple eavesdroppers," *Wireless Personal Communications*, vol. 1007, no. 10, pp. 1-26 Feb. 2017.

[13] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.,* vol. 64, no. 1, pp. 70-82, Jan. 2016.

[14] S. Jin, M. M. Mckay, C. Zhong, and K. K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory,* vol. 56, no. 5, pp. 2204-2224, Apr. 2010.

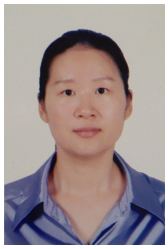
[15] S. Jin, X. Liang, K. K. Wong, X. Gao, and Q. Zhu, "Ergodic rate analysis for multipair massive MIMO two-way relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1480-1491, Nov. 2014.

[16] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Jul. 2016.

[17] Y. Zou, X. Li, and Y. C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222-2236, Nov. 2014.
[18] L. Fan, S. Jin, C. Wen, and H. Zhang, "Uplink achievable rate for massive MIMO systems with low-resolution ADC," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2186-2189, Dec. 2015.
[19] G. Pan, H. Lei, Y. Deng, L. Fan, J. Yang, Y. Chen, and Z. Ding, "On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831-3843, Sept. 2016.
[20] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna selection aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Tech.*, vol. 65, no. 1, pp. 214-225, Jan. 2015.
[21] W. Tan, M. Matthaiou, S. Jin, and X. Li, "Spectral efficiency of DFT based processing hybrid architectures in massive MIMO," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 586-589, Sep. 2017.
[22] D. Deng, L. Fan, X. Lei, W. Tan, and D. Xie "Joint User and Relay Selection for Cooperative NOMA Networks," *IEEE Access*, vol. 5, pp. 20220-20227, Sep. 2017.
[23] C. Weng and K. Psounis, "Distributed caching and small cell cooperation for fast content delivery," *The ACM International Symposium*, pp. 127-136, Jun. 2015.
[24] J. Song, H. Song, and C. Wan, "Optimal caching placement of caching system with helpers," *IEEE ICC*, pp. 1825-1830, Sep. 2015.
[25] B. Blaszczyszyn and A. Giovanidis "Optimal geographic caching in cellular networks," *IEEE ICC*, pp. 3358-3363, Jun. 2015.
[26] G. Zheng, H. A. Suraweera, and I. Krikidis, "Optimization of hybrid cache placement for collaborative relaying," *IEEE Commun. Lett.*, vol. 21, no. 2, pp. 442 - 445, Nov. 2016.
[27] A. Sengupta, R. Tandon, and T. C. Clancy, "Fundamental limits of caching with secure delivery," *IEEE Trans. Inf. Forensics Security,* vol. 10, no. 2, pp. 355-370, Feb. 2015.
[28] A. Sengupta, R. Tandon, and T. C. Clancy, "Decentralized caching with secure delivery," *IEEE Int. Symp. Inf. Theory (ISIT)* , pp. 41-45, Jun. 2014.
[29] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 752-754, Aug. 2010.
[30] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428-6443, Oct. 2011.
[31] T. Cui, F. Gao, T. Ho and A. Nallanathan, "Distributed space-time coding for two-way wireless relay networks," *IEEE Trans. Signal Process.*, vol. 57, no. 2, pp. 658-671, Feb. 2009.
[32] Z. Chen, J. Lee, and M. Kountouris, "Cooperative caching and transmission design in cluster-centric small cell networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3401-3415, Mar. 2017.
[33] M. Taghizadeh, K. Micinski, S. Biswas, C. Ofria, and E. Torng, "Distributed cooperative caching in social wireless networks," *IEEE Trans. Mobile Computing*, vol. 12, no. 6, pp. 1037-1053, Jun. 2013.

Fang Shi received the bachelor degree in School of Information Science and Technology from HaiNan Normal University in 2016. She is now a graduate student at Guangzhou University. Her research interests focus on cache storage, physical-layer secure communications and wireless cooperative communications.

Weiqiang Tan received the Ph.D. degree from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2017; The M.S. degree from Chengdu University of Information Technology, China, in 2013. From 2016 to 2017, he was a visiting Ph.D student with the School of Electronics,Electrical Engineering and Computer Science, Queens University Belfast, United Kingdom. He is currently a lecturer at the school of Computer Science and Educational Software, Guangzhou University, Guangzhou. His research interests include massive MIMO and Millimeter wave wireless communication.



Junjuan Xia received the bachelor degree from the department of computer science from Tianjin University in 2003, and obtained the master degree from the department of electronic engineering from Shantou University in 2015. Now she works for the school of Computer Science and Educational Software, Guangzhou University as a laboratory assistant. Her current research interests include wireless caching, physical-layer security, cooperative relaying and interference modeling.

Dongqing Xie received his B.Sc. in applied mathematics and M.Sc. in computer software from Xidian University, China; and received his Ph.D. in applied mathematics,from Hunan University, China. He is the Dean and a professor at the School of Computer and Education Software of Guangzhou University. He has been a visiting scholar at Nipissing University, Canada. His research interests include information security and cryptography.He is a member of CCF.

Lisheng Fan received the bachelor and master degrees from Fudan University and Tsinghua University, China, in 2002 and 2005, respectively, both from the Department of Electronic Engineering. He received the Ph.D degree from the Department of Communications and Integrated Systems of Tokyo Institute of Technology, Japan, in 2008. He is now a Professor with GuangZhou University. His research interests span in the areas of wireless cooperative communications, physical-layer secure communications, interference modeling, and system performance evaluation. Lisheng Fan has published many papers in international journals such as IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, IEEE Transactions on Information Theory, as well as papers in conferences such as IEEE ICC, IEEE Globecom, and IEEE WCNC. He is a guest editor of EURASIP Journal on Wireless Communications and Networking, and served as the chair of Wireless Communications and Networking Symposium for Chinacom 2014. He has also served as a member of Technical Program Committees for IEEE conferences such as Globecom, ICC, WCNC, and VTC.