Mobile Networks and Applications (2020) 25:1729–1735
https://doi.org/10.1007/s11036-020-01583-7

Security Aware Caching Placement Optimization Strategy in Cooperative Networks

Huiyun Xia[1] · **Xiaokang Zhou**[1] · **Cheng Li**[2]

Published online: 6 June 2020

Abstract
Caching frequently requested contents at fog nodes has been proposed to alleviate the unprecedent pressure of limited backhaul capacity and decrease latency. However, due to the broadcast characteristic of wireless communication and limited resource, how to ensure information security is of vital importance. Compared with traditional encryption method, physical layer security has advantages on low computing complexity and resource consumption. In this paper, aiming at maximizing secrecy throughput, the Wynar's encoding method is adopted to ensure communication security by jointly optimizing the caching placement strategy and secrecy rate. Numerical results have demonstrated that the proposed security aware caching placement strategy can outperform the other two baseline algorithms and achieve the tradeoff between diversity and security in cooperative networks.

Keywords Physical layer security · Probabilistic caching · Secrecy rate · Cooperative networks · Average secrecy throughput

1 Introduction

The explosively increasing traffic data as well as diverse demands of universal mobile users, resulting from the rapid development of 5G communication technologies, has brought unprecedented pressure to the backhaul links with limited capacity. The table in [1] has demonstrated the enhancement of the next-generation capabilities from IMT-2020 compared with IMT-Advanced. To alleviate such bottleneck, fog computing emerged as an efficient way to compensate for "the last mile". Caching at the fog node as a solution has received more and more attention, since it can not only reduce the pressure of backhaul links and probability of network congestion, but also decrease the network latency. However, due to the limitation of resource, caching at fog nodes also faces the challenge of being eavesdropped by illegitimate users due to its broadcast nature. Therefore, how to ensure communication confidentiality is of vital importance. Traditional encryption method sacrifices some resources to accomplish secret key management and secret key distribution and requires high computing complexity, which is not affordable for fog nodes with limited resources and computing capability. With respect to this, physical layer security has its advantage by means of channel coding and exploiting the inherent characteristics of wireless media, such as random noise and fluctuate channels.

Recently, physical layer security aided caching schemes have obtained some achievements. Considering balancing file diversity as well as file security, in [2, 3], the hybrid caching placement strategy is proposed to jointly optimize the "most popular content" and "largest content diversity" caching schemes to improve the overall secrecy throughput and secrecy energy efficiency in a static network with multiple randomly located eavesdroppers. A hybrid cache placement scheme for physical layer security in cooperative networks is analyzed in [4] by combining the traditional base station caching, most popular content caching and largest content diversity caching schemes

✉ Huiyun Xia
summerxiahy@163.com

Xiaokang Zhou
kangsenneo@sina.com

Cheng Li
licheng@mun.ca

[1] School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, 150001, People's Republic of China

[2] Electrical and Computer Engineering Faculty of Engineering and Applied Science, Memorial University, 230 Elizabeth Ave, St. John's, NL A1C 5S7, Canada

together. In [5], two transmission schemes are analyzed to secure caching-aided communication system from symbol level and bit level respectively. To better adapt to the changes of file popularity, probabilistic caching [6] is proposed. By adopting probabilistic caching strategy, the average secure delivery probability and redundant rate are jointly optimized to maximize achievable transmission rate within a stochastic network in [7]. By taking different file secrecy levels into consideration, probabilistic caching is proposed to achieve a tradeoff between secrecy and delivery in [8]. Except for the well-known Wyner's wiretap code [9], some other PHY-security technologies have been adopted to secure communication in cache-aided networks. In [10], a secure wiretap coding scheme along with physical layer key generation and authentication method is proposed to cope with the security challenges in heterogeneous IoT with multiple access mobile edge computing networks. A cache-enabled physical layer security method jointly considering transmission and caching placement is proposed in [11] to alleviate the burden of backhaul link and improve communication security by using beamforming and artificial noise design.

However, to the best of our knowledge, the above literature mainly concentrate on communication between the nearest base station and user, sacrificing the cooperative gain for security. Therefore, how to ensure communication confidentiality in a cooperative cache-aided stochastic network with physical layer method needs to be explored, which is the contribution of our work. In this paper, we consider secure communication in cooperative stochastic networks, by jointly design caching placement and secrecy rate to maximize secrecy throughput. The rest of this paper is organized as follows. The system model is described in Section 2. Section 3 analyses the optimization problem, followed by the optimization solution in Section 4 and numerical results in Section 5, and the conclusion is drawn in Section 6.

2 System model and performance matric

We consider a downlink wireless cooperative network, where all the base stations within the concerned area are capable of caching contents, as illustrated in Fig. 1. In our system model, a homogeneous Poisson point process (PPP) of density λ is adopted to describe the distribution of base stations and their locations are denoted by Φ. The base stations within communication scope (the shaded area Ω in Fig. 1) jointly transmit their cached file to the legitimate user requesting that file. Meanwhile, there exists a randomly located eavesdropper attempting to overhear the communication process.

Assuming each legitimate user can be fully supported by cooperative base stations with maximum available bandwidth. All base stations and user devices are equipped with single antenna, so is the eavesdropper. The base stations have no knowledge of the channel state information for both legitimate users as well as eavesdroppers. The capacity of caching memory for each base station is assumed to be the same, i.e., M files, with the total number of files being F ($F \geq M$). The set of file index is denoted as $\mathcal{F} = \{1, 2, \ldots, F\}$, and the size of all files is assumed to be the same, which is usually normalized to unit, without loss of generality. Assuming the popularity of files follows Zipf distribution as [6, 8], given by Eq. 1,

$$f_m = \frac{1/m^{\gamma}}{\sum_{i=1}^{F} 1/i^{\gamma}}, \qquad m \in \mathcal{F}. \tag{1}$$

γ indicates the skewness of Zipf distribution. m is the index of the requested file, and we assume a smaller index m

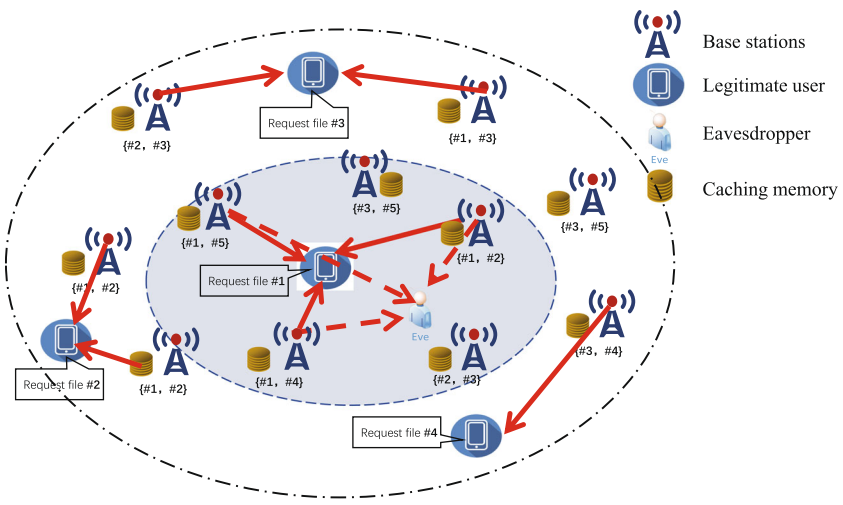

Fig. 1 The downlink file delivery process with cooperative base stations in cache aided network coexisting with an eavesdropper in the case of $F = 5$, $M = 2$

corresponds to a larger f_m. A probabilistic caching strategy is applied for the base stations to independently cache files from each other. Based on the caching probability set $P = \{p_1, p_2, ..., p_F\}$ with the constraints in Eq. 2, each base station randomly caches M files by the probabilistic caching method described in [6].

$$\begin{aligned} &\textstyle\sum_{m=1}^{F} p_m = M, \\ &0 \le p_m \le 1, \quad m \in \mathcal{F}. \end{aligned} \tag{2}$$

Without loss of generality, the legitimate user requesting file m is located at the origin of the polar coordinate $(0, 0) \in \mathcal{R}^2$, and the location of the kth base station as well as the eavesdropper is denoted as $(r_{b,k}, \theta_{b,k})$ and (r_e, θ_e), where r and θ represent the corresponding distance and angle in the polar coordinate. Therefore, the distance between the kth base station and the eavesdropper is calculated as $r_{j,k} = \sqrt{r_{b,k}^2 + r_{e,j}^2 - 2r_{b,k}r_{e,j}\cos\left(\theta_{b,k} - \theta_{e,j}\right)}$. The probability of requested file m follows (1). Besides, the base stations which cache file m can be modeled as an independent PPP with density $\lambda_m = p_m\lambda$. And we denote the locations of those base stations within Ω as Ω_m, thus $\cup_{m=1}^{F}\Omega_m = \Omega$.

When the legitimate user requests a file m , the base stations caching file m in Ω will cooperatively transmit file m to user with transmit power P_t in one time slot. The radius of Ω is R_c. The channel gains experienced are modeled as distance-based pathlosses with exponent α along with independent and identically distributed small scale fading coefficients, which are circularly symmetric complex Gaussian distributed with zero mean and unit variance. The cache hit event takes place when there exists at least one base station in Ω caching the requested file, or else the cache miss happens. We set the transmission over backhaul link aside due to the concern of latency.

The received signal to interference plus noise ratio (SINR) at the legitimate user when requesting file m is given by Eq. 3,

$$SINR_b^m = \frac{P_t|\sum_{x\in\Omega_m} x^{-\alpha/2}h_x|^2}{\sigma^2 + \sum_{y\in\Phi\setminus\Omega} y^{-\alpha}|h_y|^2}, \tag{3}$$

where x indicates the distance between the base station caching file m and the legitimate user, which is the corresponding r_b in the polar coordinate. Besides, h_x represents the small scale channel gains of base stations to the legitimate user. From (3), we can observe that the received SINR at legitimate user is dynamically affected by the caching placement strategy $\{p_m\}_{m=1}^{F}$.

Due to the random location of eavesdropper, there may exist the condition that the received SINR at eavesdropper is better than that of legitimate user. Therefore, it is necessary to adopt some measures to ensure communication confidentiality. In this paper, we adopt the Wynar's wiretap code to achieve secure communication, considering its advantage of low computational complexity and low energy consumption over traditional encryption methods and other physical layer solutions. According to the principle of wiretap code, the redundant rate denoted as R_e is embedded into the data to ensure security. Besides, the transmitted confidential data rate is denoted as R_s, which is named secrecy rate. Consequently, the transmitted data rate R_t can be expressed as $R_t = R_e + R_s$. Meanwhile, the achievable rate of the main channel (i.e., the channel between base stations and the legitimate user) under unit bandwidth when delivering file m can be calculated by $C_b^m = \log_2(1 + SINR_b^m)$.

3 Problem formulation

In order to evaluate the security performance under different caching placement strategies as well as secrecy rate, we adopt the secrecy throughput as performance criteria. Under the condition of delivering file m, the expression of secrecy throughput Φ^m is

$$\Phi^m = R_s^m P_c^m, \tag{4}$$

where, P_c^m is connection probability for delivering file m, which is calculated as $P_c^m = \mathrm{P}\{C_b^m \ge R_e^m + R_s^m|\mathcal{S}^m\}\mathrm{P}\{\mathcal{S}^m\}$. $\mathcal{S}^m$ is the cache hit event of file m, and $\mathrm{P}\{\mathcal{S}^m\} = \mathrm{P}\{|\Omega_m| \ne 0\}$. Therefore, the average network throughput Φ can be described as a weighted sum of secrecy throughput under each file's delivery and probability of each file being requested. Then, aiming at maximizing Φ, the security aware caching placement optimization problem can be formulated as (5),

$$\begin{aligned} &\max \Phi = \textstyle\sum_{m=1}^{F} f_m \Phi^m. \\ &s.t. \begin{cases} SINR_e \le \beta_e, \\ \sum_{m=1}^{F} p_m = M, \\ 0 \le p_m \le 1, \quad m \in \mathcal{F}. \end{cases} \end{aligned} \tag{5}$$

And β_e in Eq. 5 is the SINR threshold of eavesdropper recovering confidential files.

Recall the system model in part 2, the density of base stations caching file m is denoted as $\lambda_m \triangleq p_m\lambda$. Therefore, when requesting file m, the number of caching hit event follows PPP distribution with density λ_m , as shown in Eq. 6:

$$\mathrm{P}\{n = k\} = \frac{e^{-\lambda_m}{\lambda_m}^k}{k!}. \tag{6}$$

Accordingly, the cache hit probability $\mathrm{P}\{\mathcal{S}^m\}$ can be expressed by Eq. 7,

$$\begin{aligned} \mathrm{P}\{\mathcal{S}^m\} &= \mathrm{P}\{|\Omega_m| \ne 0\} \\ &= 1 - \mathrm{P}\{N = 0\} \\ &= 1 - e^{-\lambda p_m \pi {R_c}^2}. \end{aligned} \tag{7}$$

Consequently, with given communication area Ω and base station density λ, the cache hit probability is affected by the caching probabilities of different files.

On the other hand, when delivering file m, the connection probability P_c^m can be derived by Eq. 8, where, $\tau_m \triangleq 2^{R_t^m} - 1$.

$$\begin{aligned} P_c^m &= \mathrm{P}\left\{\log_2\left(1+SINR_b^m\right) \geq R_t^m | \mathcal{S}^m\right\} \mathrm{P}\{\mathcal{S}^m\} \\ &= \mathrm{P}\left\{SINR_b^m \geq \tau_m | \mathcal{S}^m\right\} \mathrm{P}\{\mathcal{S}^m\}. \end{aligned} \tag{8}$$

In the interference-limited scenario, compared with the interference power, the noise power is very small and thus can be neglected. Therefore,

$$\begin{aligned} P_c^m &= \mathrm{P}\left\{SIR_b^m \geq \tau_m | \mathcal{S}^m\right\} \mathrm{P}\{\mathcal{S}^m\} \\ &= \mathrm{P}\{P_t | \sum\nolimits_{x\in\Omega_m} x^{-\alpha/2} h_x|^2 \geq \tau_m I\} \mathrm{P}\{\mathcal{S}^m\} \\ &\overset{(a)}{=} \mathrm{E}_{x,I}[e^{(\sum_{k\in|\Omega_m|} x_k^{-\alpha})^{-1}\tau_m I}] \\ &\overset{(b)}{=} \mathrm{E}_x[\mathcal{L}_I(\frac{\tau_m}{\sum_{k=1}^K x_k^{-\alpha}})] \\ &\overset{(c)}{=} \mathrm{E}_x[e^{-sI}] \\ &= \mathrm{E}_x[e^{-s\sum_{y\in\Phi\setminus\Omega} y^{-\alpha}|h_y|^2}] \\ &= \mathrm{E}_x[\prod_{y\in\Phi\setminus\Omega} e^{-s|h_y|^2 y^{-\alpha}}] \\ &= \mathrm{E}_x[\prod_{y\in\Phi\setminus\Omega} \mathrm{E}_{|h_y|^2}[e^{-s|h_y|^2 y^{-\alpha}}]] \\ &\overset{(d)}{=} \mathrm{E}_x[\prod_{y\in\Phi\setminus\Omega} e^{\frac{1}{1+sy^{-\alpha}}}] \\ &= \mathrm{E}_x[exp(-2\pi\lambda\int_{R_c}^{+\infty} \frac{sr^{-\alpha}}{1+sr^{-\alpha}} r dr)] \\ &\overset{(e)}{=} \mathrm{E}_x[-\pi\lambda s^{\frac{2}{\alpha}} \int_{R_c^2 s^{\frac{-2}{\alpha}}}^{+\infty} \frac{1}{1+w^{\frac{\alpha}{2}}} dw]. \end{aligned} \tag{9}$$

Noticing that (a) holds for $|\sum_{x\in\Omega_m} x^{-\alpha/2}h_x|^2 \sim exp(\frac{1}{\sum_{x\in\Omega_m} x^{-\alpha}})$ and $I = \sum_{y\in\Phi\setminus\Omega} y^{-\alpha}|h_y|^2$; (b) is the Laplace transform of I; (c) holds for $s = \frac{\tau_m}{\sum_{k=1}^K x_k^{-\alpha}}$, and (d) holds for $|h_y|^2 \sim exp(1)$. When $\alpha = 4$, we can have

$$\int_{R_c^2 s^{\frac{-2}{\alpha}}}^{+\infty} \frac{1}{1+w^{\frac{\alpha}{2}}} dw = \frac{\pi}{2} - arctan(R_c^2 s^{-\frac{1}{2}}). \tag{10}$$

Substituting (10) into (9), the connection probability P_c^m is

$$P_c^m = \mathrm{E}_x[exp(-\pi\lambda(\frac{\tau_m}{\sum_{k=1}^K x_k^{-\alpha}})^{\frac{2}{\alpha}}(\frac{\pi}{2} - arctan(R_c^2 s^{-\frac{1}{2}})))]. \tag{11}$$

We mark the distance between the legitimate user and the nearest base station hitting file m is z. Therefore, $\sum_{k=1}^K x_k^{-\alpha} = z^{-\alpha} + \sum_{x\in\Omega_m\setminus z} x^{-\alpha}$. According to [12], the expectation of $D_m \triangleq \sum_{x\in\Omega_m\setminus z} x^{-\alpha}$ is given as

$$\begin{aligned} \mathrm{E}[D_m] &= \mathrm{E}[\sum_{x\in\Omega_m\setminus z} x^{-\alpha}] \\ &= 2\pi p_m \lambda \int_z^{R_c} z^{-\alpha+1} dz \\ &= \frac{2\pi p_m \lambda}{\alpha-2}(z^{2-\alpha} - R_c^{2-\alpha}). \end{aligned} \tag{12}$$

Due to the fact that $arctan(\frac{1}{x}) + arctan(x) = \frac{\pi}{2}$, and substituting (7) and (12) into (11), the final expression of P_c^m is given as

$$\begin{aligned} P_c^m = 2\pi p_m \lambda \int_0^{R_c} z exp(&-\pi\lambda s^{\frac{2}{\alpha}} arctan(R_c^{-2} s^{\frac{1}{2}}) \\ &-\pi p_m \lambda z^2) dz, \end{aligned} \tag{13}$$

where, $s = \frac{\tau_m}{z^{-\alpha} + \frac{2\pi p_m \lambda}{\alpha-2}(z^{2-\alpha} - R_c^{2-\alpha})}$.

When $R_c^{-2} s^{\frac{1}{2}} < 1$, $arctan(R_c^{-2} s^{\frac{1}{2}}) \approx R_c^{-2} s^{\frac{1}{2}}$. As a result, P_c^m can be approximated as

$$P_c^m \approx 2\pi p_m \lambda \int_0^{R_c} z exp(-\pi\lambda s^{\frac{2}{\alpha}} R_c^{-2} s^{\frac{1}{2}} - \pi p_m \lambda z^2) dz. \tag{14}$$

And substituting (14) into (4), the average secrecy throughput Φ can be derived by

$$\begin{aligned} \Phi \approx \sum_{i=1}^F 2\pi p_m \lambda f_m R_s^m \int_0^{R_c} z exp(&-\pi\lambda s^{\frac{2}{\alpha}} R_c^{-2} s^{\frac{1}{2}} \\ &-\pi p_m \lambda z^2) dz. \end{aligned} \tag{15}$$

4 Optimization strategy

From equation (15), we can observe that the average secrecy throughput dynamically varies with the transmitting data rate R_t^m (i.e. R_e^m and R_s^m) and the caching placement probabilities $\{p_m\}_{m=1}^F$. To maximize the average network throughput Φ in Eq. 5 is the same as maximizing Φ^m, since the concavity of function will not be affected by the weighted sum function. According to (4), assuming that the secrecy rate R_s^m is given, in order to maximize Φ^m, we can improve the connection probability P_c^m. Based on the definition of connection probability, $P_c^m = \mathrm{P}\{C_b^m \geq R_e^m + R_s^m | \mathcal{S}^m\} \mathrm{P}\{\mathcal{S}^m\}$, the more base stations participate in transmission cooperation, the larger P_c^m is, which means the probabilities of different files should be distinct. However, when the probabilities of different files are distinctly different, $\mathrm{P}\{\mathcal{S}^m\}$ is lower according to (7), corresponding to less diversity. Therefore, there exists a tradeoff between the

connection probability and cache hit probability under given transmitting data rate.

Similarly, there is another tradeoff under fixed caching probability. With given caching probability, $\mathrm{P}\{\mathcal{S}^m\}$ is fixed. Denoting $\omega^m \triangleq R_s^m \mathrm{P}\{C_b^m \geq R_e^m + R_s^m | \mathcal{S}^m\}$, thus both the redundant rate R_e^m and secrecy rate R_s^m can influence ω^m. However, R_e^m can only affect P_c^m. Therefore, in order to maximize ω^m, we need to set R_e^m as small as possible. On the other hand, to make sure of secure communication, the constraints $SINR_e^m \leq \beta_e^m$ leads to the optimal value of R_e^m being $R_e^0 \triangleq \log_2(1 + SINR_e^m)$. Hence, with the given caching probability and optimal redundant rate, to improve secrecy throughput, the secrecy data rate R_s^m should be improved. However, the larger R_s^m will lead to a smaller P_c^m. Therefore, our optimization goal is to find an optimal caching probability and secrecy rate to balance the tradeoffs and achieve an optimal average secrecy throughput performance.

The optimization problem in Eq. 5 is proved to be a non-convex problem. To simplify the optimization problem, a two-stage solution is proposed based on the above analysis to jointly optimize P_c^m and R_s^m. The first stage is to optimize $\{p_m\}_{m=1}^F$ for maximizing P_c^m with fixed R_s^m. When R_c is large enough, s can be approximated as $s = \frac{\tau_m}{\pi p_m \lambda z^{-2}}$. Hence, P_c^m can be further approximated by

$$\begin{aligned} P_c^m &\approx 2\pi p_m \lambda \int_0^{R_c} z e^{(\frac{-\tau_m}{R_c^2 p_m} - \pi p_m \lambda) z^2} dz \\ &= \frac{\pi p_m^2 \lambda R_c^2}{\pi p_m^2 \lambda R_c^2 + \tau_m}. \end{aligned} \tag{16}$$

Therefore, (15) can be simplified as (17),

$$\Phi = \sum_{m=1}^{F} f_m R_s^m \frac{\pi \lambda R_c^2 p_m^2}{\pi \lambda R_c^2 p_m^2 + \tau_m}. \tag{17}$$

By analyzing the second derivative of Φ, we can solve the optimization problem in two cases. And by adopting Lagrangian method [13], the optimized probability, denoted as $\{p_m^{opt}\}_{m=1}^F$, can be derived by

$$p_m^{opt} = min\{[\frac{\sqrt{\frac{2\sqrt{z} - \sqrt[3]{z_1} - \sqrt[3]{z_2}}{3}} - \sqrt{\frac{\sqrt[3]{z_1} + \sqrt[3]{z_2}}{3}}}{4\pi\lambda R_c^2}]^+, 1\}, \tag{18}$$

where, $z_{1,2} = \frac{-3B \pm 3\sqrt{B^2 - 4AC}}{2}$, $z = (\sqrt[3]{z_1} + \sqrt[3]{z_2})^2 - 3A$. And $A = 192\pi\lambda\tau_m R_c^2$, $B = 72\pi\lambda R_c^2 t$, $C = -64\pi\lambda\tau_m R_c^2$, $t = \sqrt{\frac{2\pi\lambda\tau_m f_m R_c^2}{w + \mu_m}}$.

Based on the given $\{p_m^{opt}\}_{m=1}^F$, we then optimize R_s^m by maximizing Φ^m, assuming all files have identical secrecy rate. Set the first derivation of Eq. 17 to zero and the optimized secrecy rate R_s^{opt} can be derived by

$$\frac{d\Phi^m}{dR_s^m} = 0. \tag{19}$$

Substituting (4) and $\tau \triangleq 2^{R_s + R_e^0} - 1$ into (19), R_s^{opt} can be derived by

$$\lambda\pi R_c^2 p_m^2 + 2^{R_e^0 + R_s^{opt}}(1 - ln2 R_s^{opt}) = 0. \tag{20}$$

Due to the complexity of Eq. 20, we can use bisection method to get R_s^{opt}. The pseudo-code is shown in Algorithm 1. Accordingly, we iteratively optimize the problem following (16) and (19) until achieving the maximization of the average network throughput Φ^{opt}.

Algorithm 1 Using bisection method to calculate R_s^{opt} with given p_m.

Require: R_s^{opt}

Ensure: $\lambda, \pi, R_c, p_m, R_e^0$, objective function $f(x)$ and tolerance error ϵ.

```
Initialize the iterative number i = 0, and set a = 0, b = 10;
repeat
    if f((a+b)/2) > 0 then
        b = (a+b)/2;
    else
        a = (a+b)/2.
    end if
until (b−a)/2 < ε return R_s^opt = (a+b)/2.
```

5 Numerical analysis

In this section, we evaluate the performance of the proposed security aware caching placement optimization strategy, with respect to the successful connection probability and average network secrecy throughput. The settings of simulation parameters are depicted as Table 1.

The successful connection probability is analyzed in Fig. 2 to validate the theoretical results by evaluating different communication radius R_c and different secrecy rate R_s. From Fig. 2, we can observe that the theoretical successful connection probability results derived in (15) matches well with the Monte-Carlo simulation results, especially when R_c is small comparing with Φ. Besides, the approximation results in (16) can well depicts the tendency of successful connection probability, too. With

Table 1 Parameter settings of simulation

Parameter	Symbol	Value
transmitting power	P_t	37dBm
base station density	λ	10^{-4} units/m^2
pathloss exponent	α	4
radius of considering area Φ	d	1000m

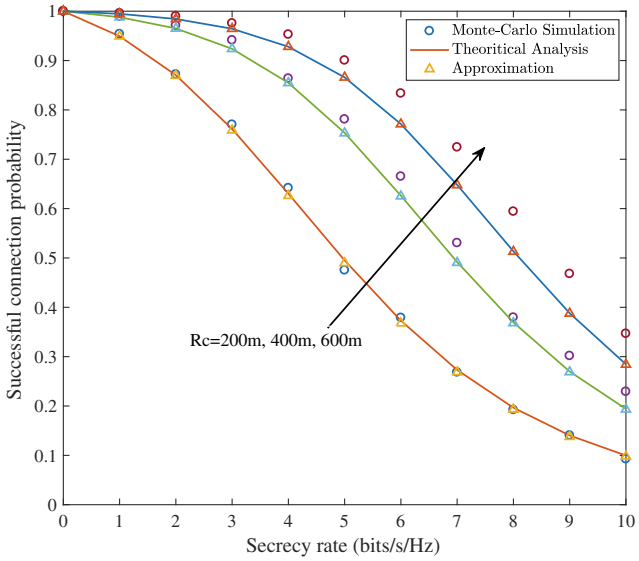

Fig. 2 The successful connection probability P_c under different secrecy rates R_s and communication radius R_c, with given probabilistic caching scheme $M = 1, F = 1, \gamma = 1$

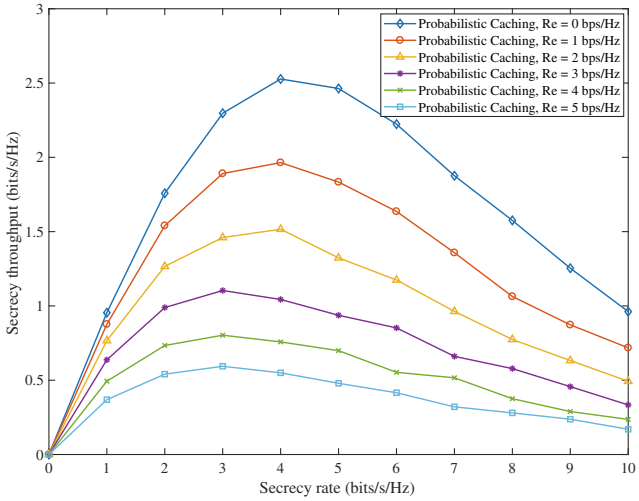

Fig. 4 The relationship between secrecy throughput Φ and secrecy rate R_s under different redundant rate R_e

fixed secrecy rate, a larger communication radius leads to a larger successful connection probability. That's because the larger communication radius means more base stations can participate in file delivery cooperation, thus can improve the signal to interference plus noise ratio at the legitimate receiver, assuming that the communication security can be guaranteed by adopting a proper redundant rate. And the successful connection probability decreases as the secrecy rate increases, which is consistent with (15).

Figure 3 compares the optimal probabilistic caching scheme with two baseline schemes, namely, the uniform caching scheme and the most popular file (MPF) caching scheme under different file popularity skewness parameter γ, when the total file amount is 5 and caching capacity is 2. The P_c of MPF caching and optimal probabilistic caching varies from different skewness parameters while the P_c of uniform caching remains unchanged, because the caching probabilities of uniform caching don't depend on file popularity while the other two caching schemes do. On the other hand, the optimal probabilistic caching scheme always performs better than the other baseline schemes. Besides, when the skewness parameter is high, MPF caching scheme is closer to the proposed optimal probabilistic caching scheme, and vice versa for a low skewness parameter. The reason is that the caching probabilities in probabilistic is more flexible and thus can better adjust to the change of file popularity than the other two baseline schemes.

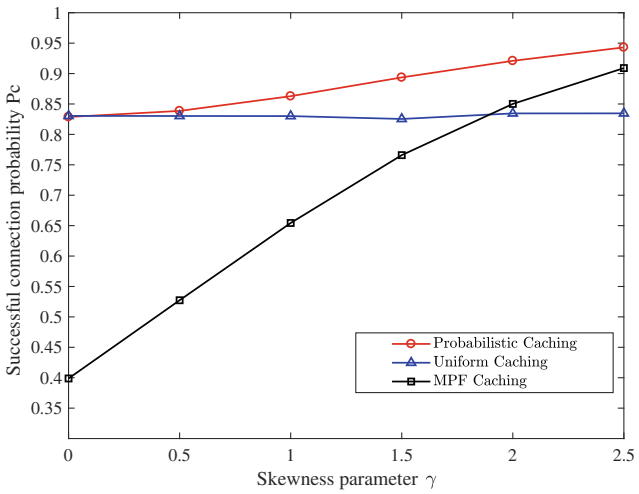

Fig. 3 The successful connection probability comparison of three caching schemes, i.e., Uniform caching, MPF caching and optimal probabilistic caching scheme, under different skewness parameter γ of file popularity when $M = 2, F = 5$

The relationship between secrecy throughput Φ and secrecy rate R_s is evaluated in Fig. 4 under different redundant rate R_e. From Fig. 4 we can draw a conclusion that with the increase of R_s, Φ first increases to a maximum value and then decreases, which means we can find an optimal secrecy rate to maximize the average secrecy throughput. On the other hand, the larger redundant rate will lead to a smaller average secrecy throughput, due to the connection probability decreases as R_e increases. Therefore, the stronger the decoding capability of eavesdropper, the worse the secrecy throughput performance is.

6 Conclusions

This paper has investigated joint optimization of physical layer security and caching placement strategy in a cooperative

network with randomly distributed base stations, coexisting with a randomly located eavesdropper. We first describe the cooperative communication system model. Then, the caching placement strategy is analyzed by adopting stochastic geometry to deal with the connection probability. With the purpose of maximizing average secrecy throughput, the redundant rate is embedded into the transmitted data and the caching probability and secrecy rate are iteratively optimized by our proposed algorithm. The numerical analysis has validated our theoretical analysis and the outperformance of the proposed algorithm over the other two baseline algorithms has been demonstrated.

References

1. Han S, Zhang Y, Meng W, Zhang Z (2018) "Precoding Design for Full-Duplex Transmission in Millimeter Wave Relay Backhaul". Mobile Netw Appl 23(5):1416–8C1426
2. Zheng TX, Wang HM, Yuan JH (2018) Physical-Layer Security in Cache-Enabled cooperative small cell networks against randomly distributed eavesdroppers. IEEE Trans Wirel Commun 17(9):5945–5958
3. Zheng TX, Wang HM, Yuan JH (2018) Secure and Energy-Efficient transmissions in Cache-Enabled heterogeneous cellular networks: performance analysis and optimization. IEEE Trans Commun 66(11):5554–5567
4. Shi F, Tan W, Xia J, Xie D, Fan L, Liu X (2018) Hybrid cache placement for Physical-Layer security in cooperative networks. IEEE Access 6:8098–8108
5. Zhao W, Chen Z, Li K, Liu N, Xia B, Luo L (2018) Caching-Aided Physical layer security in wireless Cache-Enabled heterogeneous networks. IEEE Access 6:68920–68931
6. Blaszczyszyn B, Giovanidis A (2015) "Optimal geographic caching in cellular networks". In: 2015 IEEE International Conference on Communications ICC, pp 3358–3363
7. Zhang S, Sun W, Liu J, Kato N (2019) Physical layer security in large scale probabilistic caching: analysis and optimization. IEEE Commun Lett 23:1–1
8. Yang Q, Wang H, Zheng T (2018) Delivery-Secrecy Tradeoff for Cache-Enabled stochastic networks: content placement optimization. IEEE Trans Veh Technol 67(11):11309–11313
9. Csiszar I, Korner J (1978) Broadcast channels with confidential messages. IEEE Trans Inf Theory 24(3):339–348
10. Wang D, Bai B, Lei K, Zhao WB, Yang YP, Han Z (2019) Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. IEEE Access, Article 7:54508–54521
11. Xiang L, Ng DWK, Schober R, Wong VWS (2018) Cache-Enabled Physical layer security for video streaming in Backhaul-Limited cellular networks. IEEE Trans Wirel Commun 17(2):736–751
12. Chae SH, Quek TQS, Choi W (2017) Content placement for wireless cooperative caching helpers: a tradeoff between cooperative gain and content diversity gain. IEEE Trans Wirel Commun 16(10):6795–6807
13. Han S, Zhang Y, Meng W, Chen H-H (2018) Self-Interference-Cancelation-Based SLNR Precoding design for Full-Duplex Relay-Assisted system. IEEE Trans Veh Technol 67(9):8249–8262