Secure Probabilistic Caching for Stochastic Multi-User Multi-Relay Networks

Lisheng Fan[1], Xianfu Lei[2], Nan Zhao[3], Pingzhi Fan[2], and George K. Karagiannidis[4]
[1]School of Computer Science, Guangzhou University, Guangzhou, China.
[2]Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, China.
[3]School of Information and Communication Engineering, Dalian University of Technology, China.
[4]Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Greece.
(E-mails: lsfan@gzhu.edu.cn, xflei@home.swjtu.edu.cn, zhaonan@dlut.edu.cn, p.fan@ieee.org, geokarag@auth.gr).

***Abstract*—In this paper, we study a stochastic multi-user multi-relay network, where the data transmission can be overheard by multiple eavesdroppers. The users, relays and eavesdroppers are assumed to arrive at the network subject to homogeneous poisson point process (PPP). Cache equipped at the relays and users can pre-store part of file contents, which can help enhance the transmission security. Hence, it is of vital importance to design an effective secure probabilistic caching strategy to ensure the security of content transmission. To this end, we first consider several cache-aided transmission modes of self-fetch, D2D-transmission, relay-transmission, and source-transmission. We then study the network secrecy performance by analyzing the expression of secure cache throughput and an analytical lower bound. In order to maximize the secure cache throughput, we further optimize the probabilistic caching strategy by using a heuristic algorithm. Numerical results are provided to demonstrate that the proposed strategy outperforms the conventional caching strategies.**

I. Introduction

In accordance with the great progress in wireless big data, many wireless techniques have been recently devised to tackle with this challenge. Wireless caching is one of the most promising techniques, since it can reduce the data traffic load by storing contents closer to the end users during non-peak time [1]–[3]. There are two fundamental cache strategies, i.e., the most popular contents (*MPC*) and the largest content diversity (*LCD*) strategies, which achieve the largest signal cooperation gain and the largest content delivery gain, respectively. From these two strategies, researchers extend to devise a hybrid cache strategy, in order to achieve a fine balance between signal cooperation gain and caching diversity gain [4], [5]. Different from these caching strategies, the probabilistic content caching is more proper for stochastic networks, where the nodes are randomly distributed [6]. The authors in [7] investigated a stochastic network, where the nodes are assumed to arrive by following the poisson point process (PPP), and studied the effect of probabilistic caching on network performance.

X. Lei is the corresponding author of this paper.

This work was supported by the NSF of China (Nos. 61871139/61501382/61871065/61801132), by the Guangdong Natural Science Funds for Distinguished Young Scholar (No. 2014A030306027), by the Science and Technology Program of Guangzhou (No. 201807010103), by the Fundamental Research Funds for the Central Universities (No. 2682018CX27), and by the Sichuan Science and Technology Program (No. 2017HH0035).

Due to the broadcast nature of wireless transmission, the severe issue of information leakage also arises when eavesdroppers exist in the cache-aided network, and hence it is of vital importance to study the physical-layer security to guarantee the transmission secrecy [8], [9]. In recent years, researchers begin to study the secure transmission of the cache-aided networks. The authors in [10] analyzed the problem of secure transmission of cache strategy, with the presence of one eavesdropper. In [11], unmanned aerial vehicles (UAVs) assisted security transmission for scalable videos in hyper-dense networks via caching was studied. In [12], the authors designed and optimized a hybrid caching placement in a wireless caching network to suppress the wiretap by the eavesdroppers.

In this paper, we consider a stochastic network, where the relays, users and eavesdroppers follow homogenous PPP, and caching is performed at the relays and users, which can pre-store part of file contents. The caching strategy needs to be designed, in order to ensure the security of content transmission. To this end, we first consider several cache-aided transmission modes of self-fetch, D2D-transmission, relay transmission, and source-transmission. The secure cache throughput is then used as the main performance metric based on the cache hit probability and the probability of successful transmission. We present an integral-form expression as well as an analytical lower bound for the secure cache throughput. To maximize the secure cache throughput, the heuristic algorithm is further used to optimize the probabilistic caching strategy, in order to find the optimal solution of cache placement. Numerical results are finally provided to demonstrate that the proposed probabilistic caching strategy outperforms the conventional MPC and equal probability content (EPC) cache strategies, and the network secrecy performance can be improved by increasing the cache size and density of the relays and users, or by decreasing the density of eavesdroppers.

II. System Model

As shown in Fig.1, we consider a cache-aided stochastic relay network, which comprises one source S, multiple cache-aided decode-and-forward (DF) relays $\{R_k|k = 1, 2, \ldots, K\}$, multiple legitimate users $\{u_m|m = 1, 2, \ldots, M\}$, and multiple eavesdroppers $\{E_l|l = 1, 2, \ldots, L\}$ which can overhear

978-1-5386-6119-2/18/$31.00 ©2018 IEEE

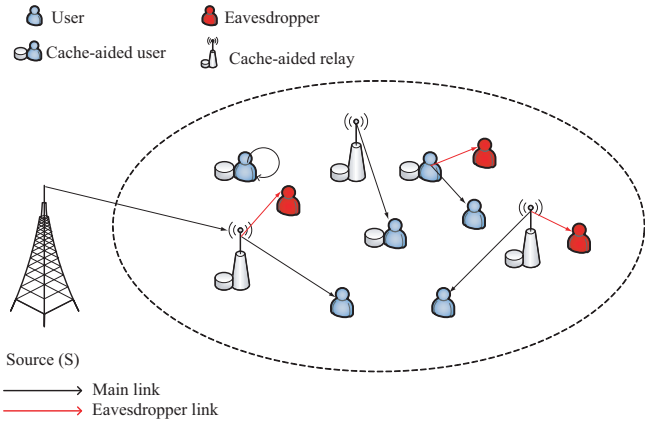

Fig. 1. System model of cache-aided stochastic relay networks

the secure messages and bring out the issue of information wiretap. The relays, users, and eavesdroppers are modeled by a homogeneous PPP Φ_r, Φ_u and Φ_e, with density of λ_r, λ_u and λ_e, respectively. As only part of users have the caching capability, we use μ ($\mu \in [0,1]$) to represent the proportion of cache-enabled users. Accordingly, the cache-enabled users also follow a homogeneous PPP with density $\mu\lambda_u$.

Due to severe shadowing, the direct links from the source to the users do not exist, and the transmission from the source to the users is performed only via relays. Moreover, all nodes in the network are equipped with a single antenna due to the size limitation [1], and all links experience Rayleigh flat fading. For a random legitimate user u_m, if the requested content can be found in the surrounding users or relays, the nearest user or relay directly forwards the content to u_m; otherwise, the content has to be transmitted from the source S to the users with the help of relays.

A. Cache Strategy

Let N denote the number of file contents requested by the users, and all the contents have the same size. The contents are characterized by their popularity, namely, the probability that the content is requested by the users. Without loss of generality, contents are ordered according to the request probability f_n, $f_1 \geq f_2 \geq \ldots \geq f_N$, and $\sum_{n=1}^{N} f_n = 1$ $(1 \leq n \leq N)$. We use the Zipf distribution to model the request probability of the popular contents, where the Zipf parameter γ represents the popularity skewness [1].

Due to the storage limitation, users and relays can not cache all of the popular contents. Hence, users and relays need to judiciously choose which content to cache. Due to the randomness of users and relays, we use the probabilistic caching strategy to place the contents on the stochastic network nodes. We use $\mathbf{q}^r = [q_1^r, \ldots, q_i^r, \ldots, q_N^r]$ and $\mathbf{q}^u = [q_1^u, \ldots, q_i^u, \ldots, q_N^u]$ to denote the cache parameters at the relays and users, respectively, where $q_i^r \in [0,1]$ and $q_i^u \in [0,1]$ represent the proportion of relays and users caching the i-th content ($i \in [1,N]$), respectively. Due to the storage limitation, we have

$$\sum_{i=1}^{N} q_i^r \leq C_R, \tag{1}$$

$$\sum_{i=1}^{N} q_i^u \leq C_U, \tag{2}$$

where C_R and C_U denote the cache size at the relays and users, respectively.

B. Transmission Modes

According to the storage location of the requested content, four cache-aided transmission modes are considered in this paper, as follows,

1) Self-fetch: When a content request occurs, the user u_m first finds in its local memory and checks whether the requested content has been stored in its cache or not. If the u_m has cached the requested content in its local memory, the request will be satisfied immediately by itself; otherwise, the following transmission modes will be used.

2) D2D-transmission: If the user u_m does not store the requested content in its local memory, u_m turns to find the file among the nearby cache-enabled users within a radius R_u. If there are multiple cache-enabled users which have already stored the requested content, the request will be met and the data is transmitted from the nearest cache-enabled user to the u_m; otherwise, the following relay-transmission and source-transmission will be used for the data transmission.

3) Relay-transmission: If the requested content has not been cached in the nearby cache-enabled users within a radius R_u, the user u_m turns to find the file among the nearby relays within a radius R_r, where $R_r > R_u$. If there are multiple relays which have stored the requested content, the request will be satisfied and the requested content will be transmitted from the nearest relay to the user; otherwise, the following source-transmission will be used for the data transmission.

4) Source-transmission: If the requested content has not been cached in the cache-enabled users or relays, it should be forwarded from the source to the u_m. In this case, as source has no direct links with users, the source firstly transmits its content to the nearest relay R_k^m, and then R_k^m decodes and forwards the content to the u_m using the same code book as the source to R_k^m.

In this paper, we mainly focus on the first three transmission modes, and study the impact of secure caching on the network secrecy performance. The impact of the source-transmission mode on the network security will be studied in our future works.

III. Performance Analysis

In this section, we use the secure cache throughput as the metric to measure the system performance of proposed cache strategy, based on the cache hit probability and probability of successful transmission. Both integral-form expression and

[1]If multiple antennas are equipped at the nodes, the secure beamforming technique can be used to enhance the network security, which will be investigated in our future work.

the associated analytical lower bound of the secure cache throughput are provided.

A. Cache Hit Probability

The cache hit probability is defined as the probability that the user u_m can successfully find the requested content in a given area within the radius R. According to the stochastic geometry, the expected number of nodes in a given area within the radius R is calculated as [6], [7]

$$E[N_e] = \lambda \pi R^2. \tag{3}$$

As the users and relays caching the i-th content follow the PPP with density $q_i^u \mu \lambda_u$ and λ_r, respectively, the associated expected number of users and relays caching the i-th content in a given area within the radius R_u and R_r is computed as [6], [7]

$$E[U] = q_i^u \mu \lambda_u \pi R_u^2, \tag{4}$$
$$E[K] = q_i \lambda_r \pi R_r^2. \tag{5}$$

From [13], the probability that there are n nodes in the area A within the radius r for a PPP distribution with density λ is

$$P(n, r) = \frac{[\lambda \pi r^2]^n}{n!} e^{-\lambda L(A)}. \tag{6}$$

Therefore, if the random user u_m is located at the origin, the probability that at least one nearby user and relay have cached the i-th content within the radius R_u and R_r is respectively given by

$$P_{f,i}^u = 1 - e^{-\pi \mu q_i^u \lambda_u R_u^2}, \tag{7}$$
$$P_{f,i}^r = 1 - e^{-\pi q_i^r \lambda_r R_r^2}. \tag{8}$$

B. Probability of Successful Transmission

According to the several cache-aided transmission modes, we analyze the probability of successful transmission in the following cases,

1) Self-fetch: For the random user u_m, if the requested content has been cached in the user's local memory, the request would be satisfied by itself. Therefore, the probability of successful transmission is equal to one.

2) D2D-transmission: If the requested content has not been cached in the user's local memory or the u_m does not have the caching ability, u_m turns to find the content among the nearby cache-enabled users within a radius R_u. When M cache-enabled users have stored the requested content, the request will be met and the data is transmitted from the nearest cache-enabled user u_t ($t \in [1, M]$) to u_m.

Therefore, when u_m broadcasts the file request to the around users, the nearest user u_t which has cached the requested content directly transmits the content to the u_m. The received signal-to-noise ratios (SNRs) at the u_m and a random eavesdropper e_l are

$$\mathsf{SNR}_{u_m}^u = \rho_1 \eta_{u_m}^u, \tag{9}$$
$$\mathsf{SNR}_{e_l}^u = \rho_1 \eta_{e_l}^u, \tag{10}$$

where $\rho_1 = P_u/\sigma^2$, $\eta_{u_m}^u = |h_{u_t,u_m}|^2 (r_{m,i}^u)^{-\alpha}$, and $\eta_{e_l}^u = |h_{u_t,e_l}|^2 (r_{u_t,e_l}^u)^{-\alpha}$. In these notations, P_u is the transmit power at the users, σ^2 is the noise variance at the receiver, $h_{i,j}$ denotes the channel parameter of the $i \to j$ link, $r_{i,j}$ is the distance from node i to j, and $r_{m,i}^u$ and r_{u_t,e_l}^u represent the distance from the u_m to the nearest u_t and e_l, respectively.

From eqs. (9) and (10), the probability of successful transmission of the secure D2D-transmission is written by

$$P_{suc,i}^u = \Pr\left\{ \log_2 \left(\frac{1 + \mathsf{SNR}_{u_m}^u}{1 + \sum_{e_l \in \Phi_e} \mathsf{SNR}_{e_l}^u} \right) > R_s \right\}, \tag{11}$$

where R_s is a given target secrecy rate and Φ_e denotes the set of eavesdroppers. In (11), the worst case of wiretap is considered, namely, the eavesdroppers can cooperate to jointly receive and decode contents through the maximum ratio combining (MRC) reception. We can rewrite (11) as

$$\begin{aligned} P_{suc,i}^u &= \Pr\left\{ \log_2 \left(\frac{1 + \rho_1 \eta_{u_m}^u}{1 + \rho_1 \sum_{e_l \in \Phi_e} \eta_{e_l}^u} \right) > R_s \right\} \qquad (12) \\ &= \Pr\left\{ \eta_{u_m}^u > \frac{\tau - 1}{\rho_1} + \tau \eta_e^u \right\} \\ &= \int_0^\infty \int_{\frac{\tau-1}{\rho_1} + \tau y}^\infty f_{\eta_{u_m}^u}(x) dx f_{\eta_e^u}(y) dy \qquad (13) \end{aligned}$$

where $\tau = 2^{R_s}$, $\eta_e^u = \sum_{e_l \in \Phi_e} \eta_{e_l}^u$, $f_{\eta_{u_m}^u}(x)$ and $f_{\eta_e^u}(x)$ denote the probability distribution functions (PDFs) of $\eta_{u_m}^u$ and η_e^u, respectively. By using the result in [14], and then applying the PDF of $\eta_{u_m}^u$ as $f_{\eta_{u_m}^u}(x) = (r_{m,i}^u)^\alpha e^{-(r_{m,i}^u)^\alpha x}$, we can calculate $P_{suc,i}^u$ as

$$\begin{aligned} P_{suc,i}^u &= E_{r_{m,i}^u} \left[e^{-\frac{(r_{m,i}^u)^\alpha (\tau-1)}{\rho_1}} \int_0^\infty e^{-\tau (r_{m,i}^u)^\alpha y} f_{\eta_e^u}(y) dy \right] \\ &\overset{(a)}{=} E_{r_{m,i}^u} \left[e^{-\frac{(r_{m,i}^u)^\alpha (\tau-1)}{\rho_1}} \mathcal{L}_{\eta_e^u}(\tau (r_{m,i}^u)^\alpha) \right], \qquad (14) \end{aligned}$$

where E_r is the expectation of distance, and the operation in (a) is the Laplace transform of η_e^u, denoted by $\mathcal{L}_{\eta_e^u}(s)$. From [14], we have

$$\begin{aligned} \mathcal{L}_{\eta_e}(s) &= \exp\left(-\lambda_e \pi \Gamma(1 + \frac{2}{\alpha}) \Gamma(1 - \frac{2}{\alpha}) s^{\frac{2}{\alpha}} \right) \\ &= \exp\left(-\beta s^{\frac{2}{\alpha}} \right), \qquad (15) \end{aligned}$$

where $\beta = \lambda_e \pi \Gamma(1 + \frac{2}{\alpha}) \Gamma(1 - \frac{2}{\alpha})$. Thus, we can further rewrite $P_{suc,i}^u$ as

$$\begin{aligned} P_{suc,i}^u &= E_{r_{m,i}^u} \left[e^{-\frac{(r_{m,i}^u)^\alpha (\tau-1)}{\rho_1}} e^{-\beta \tau^{\frac{2}{\alpha}} (r_{m,i}^u)^2} \right] \\ &= \int_0^{R_u} \exp\left\{ -\beta \tau^{\frac{2}{\alpha}} r^2 - \frac{\tau - 1}{\rho_1} r^\alpha \right\} f_{r_{m,i}^u}(r) dr, \qquad (16) \end{aligned}$$

where $f_{r_{m,i}^u}(r)$ is the PDF of $r_{m,i}^u$. From [14], we obtain the PDF of the distance from the origin to the nearest node in a PPP network as

$$f(r) = \frac{2\pi\lambda r}{1 - e^{-\pi \lambda R_{max}^2}} e^{-\pi \lambda r^2} \qquad 0 \le r \le R_{max}, \tag{17}$$

where R_{max} is the maximum distance. As the density of users that have cached the i-th content is $\mu q_i^u \lambda_u$, the PDF of $r_{m,i}^u$ is given by

$$f_{r_{m,i}^u}(r) = \frac{2\pi\mu q_i^u \lambda_u r}{1 - e^{-\pi\mu q_i^u \lambda_u R_u^2}} e^{-\pi\mu q_i^u \lambda_u r^2}, \tag{18}$$

where $0 \leq r \leq R_u$. Submitting (18) in (16), the probability of successful transmission of the secure D2D-transmission is finally obtained as

$$\begin{aligned} P_{suc,i}^u &= \int_0^{R_u} \frac{2\pi\mu q_i^u \lambda_u r}{1 - e^{-\pi\mu q_i^u \lambda_u R_u^2}} \\ &\quad \times \exp\left\{-(\beta\tau^{\frac{2}{\alpha}} + \pi\mu q_i^u \lambda_u) r^2 - \frac{\tau - 1}{\rho_1} r^\alpha\right\} dr \\ &= G(\mu q_i^u \lambda_u, \rho_1, R_u), \end{aligned} \tag{19}$$

where the $G(\lambda, \rho, R)$ function is

$$\begin{aligned} G(\lambda, \rho, R) &= 2\pi\lambda / (1 - e^{-\pi\lambda R^2}) \\ &\times \int_0^R r \exp\left\{-(\beta\tau^{\frac{2}{\alpha}} + \pi\lambda) r^2 - \frac{\tau - 1}{\rho} r^\alpha\right\} dr. \end{aligned} \tag{20}$$

3) Relay-transmission: If the requested content has not been cached in the nearby cache-enabled users within the radius R_u, u_m turn to find the file among the nearby relays within tge radius R_r. If the requested content has been cached in the nearest R_k^m, the request will be satisfied and the data is transmitted from R_k^m. The associated received SNRs at the user u_m and the eavesdropper e_l are given by

$$\mathsf{SNR}_{u_m}^r = \rho_2 \eta_{u_m}^r, \tag{21}$$

$$\mathsf{SNR}_{e_l}^r = \rho_2 \eta_{e_l}^r, \tag{22}$$

where $\rho_2 = P_r/\sigma^2$, $\eta_{u_m}^r = |h_{R_k^m, u_m}|^2 (r_{m,i}^r)^{(-\alpha)}$, and $\eta_{e_l}^r = |h_{R_k^m, e_l}|^2 (r_{R_k^m, e_l}^r)^{-\alpha}$. In these notations, P_r is the transmit power at the relays, $r_{m,i}^r$ and $r_{R_k^m, e_l}^r$ represent the distance from the nearest R_k^m to the u_m and the eavesdropper e_l, respectively.

Similar to the derivation process of $P_{suc,i}^u$ for the secure D2D-transmission, the probability of successful transmission of the secure relay-transmission is obtained as

$$\begin{aligned} P_{suc,i}^r &= \int_0^{R_r} \frac{2\pi q_i^r \lambda_r r}{1 - e^{-\pi q_i^r \lambda_r R_r^2}} e^{-\frac{(\tau-1) r^\alpha}{\rho_2}} e^{-\left(\beta\tau^{\frac{2}{\alpha}} + \pi q_i^r \lambda_r\right) r^2} dr \\ &= G(q_i^r \lambda_r, \rho_2, R_r). \end{aligned} \tag{23}$$

C. Secure Cache Throughput

From the derived expressions of cache hit probability and probability of successful transmission, we further provide the expression of the secure cache throughput as well as the analytical lower bound.

1) Integral Form: When the user u_m broadcasts the file request, the requested content may be found in several kinds of local memory, including the cache memory of the user itself, other users' cache memory and relays' cache memory. According to the file popularity and the possible transmission modes of the requested content, the secure cache throughput of the probabilistic caching strategy is written as

$$\begin{aligned} T_s &= \sum_{i=1}^N f_i \{\mu [q_i^u * 1 + (1 - q_i^u) \\ &\quad \times \left(P_{f,i}^u P_{suc,i}^u + (1 - P_{f,i}^u) P_{f,i}^r P_{suc,i}^r\right)] \\ &\quad + (1 - \mu) \left(P_{f,i}^u P_{suc,i}^u + (1 - P_{f,i}^u) P_{f,i}^r P_{suc,i}^r\right)\} \\ &= \sum_{i=1}^N f_i \Big\{\mu q_i^u + (1 - \mu q_i^u) \big[P_{f,i}^u P_{suc,i}^u \\ &\quad + (1 - P_{f,i}^u) P_{f,i}^r P_{suc,i}^r\big]\Big\}. \end{aligned} \tag{24}$$

Substituting (19) and (23) in (24), the secure cache throughput T_s is obtained as

$$\begin{aligned} T_s &= \sum_{i=1}^N f_i \Big\{\mu q_i^u + (1 - \mu q_i^u) \Big[\left(1 - e^{-\pi\mu q_i^u \lambda_u R_u^2}\right) \\ &\quad \times G(\mu q_i^u \lambda_u, \rho_1, R_u) + e^{-\pi\mu q_i^u \lambda_u R_u^2} \\ &\quad \times \left(1 - e^{-\pi q_i^r \lambda_r R_r^2}\right) G(q_i^r \lambda_r, \rho_2, R_r)\Big]\Big\}, \end{aligned} \tag{25}$$

following the constraints of

$$\begin{cases} \sum_{i=1}^N q_i^u \leq C_U, \\ \sum_{i=1}^N q_i^r \leq C_R, \\ q_i^u \in [0,1], \qquad i \in [1, N] \\ q_i^r \in [0,1], \qquad i \in [1, N] \end{cases}. \tag{26}$$

Note that since the $G(\lambda, \rho, R)$ function is an integral-form, the obtained T_s in (25) is also an integral-form, and hence it involves some computational load to compute.

2) Analytical Lower Bound: To reduce the computational complexity of T_s, we turn to present the analytical lower bound of the secure cache throughput. To this end, we first rewrite the secure cache throughput as

$$T_s = \sum_{i=1}^N f_i \left\{\mu q_i^u + \theta_i\right\}, \tag{27}$$

where θ_i is given by

$$\begin{aligned} \theta_i &= (1 - \mu q_i^u) \left[P_{f,i}^u G(\mu q_i^u \lambda_u, \rho_1, R_u)\right. \\ &\quad \left. + (1 - P_{f,i}^u) P_{f,i}^r G(q_i^r \lambda_r, \rho_2, R_r)\right]. \end{aligned} \tag{28}$$

As one can find that θ_i increases with larger value of the G function, we turn to find the lower bound of the G function, given by

$$\begin{aligned} G(\lambda, \rho, R) &\geq \exp\left(-\frac{\beta\tau^{\frac{2}{\alpha}} \left[1 - e^{-\pi\lambda R^2}(1 + \pi\lambda R^2)\right]}{\pi\lambda \left(1 - e^{-\pi\lambda R^2}\right)}\right) \\ &\times \exp\left(-\frac{(\tau - 1)(\pi\lambda)^{-\frac{\alpha}{2}} \gamma\left(\frac{\alpha}{2} + 1, \pi\lambda R^2\right)}{\rho \left(1 - e^{-\pi\lambda R^2}\right)}\right), \end{aligned} \tag{29}$$

where the proof is given in Appendix A. From the lower bound of $G(\lambda, \rho, R)$, the lower bound of θ_i is obtained in (30), as shown at the top of the next page.

$$\theta_i^{lb} = (1-\mu q_i^u)\Bigg[P_{f,i}^u \exp\Bigg(-\frac{\beta\tau^{\frac{2}{\alpha}}\left[1-e^{-\pi\mu q_i^u\lambda_u R_u^2}(1+\pi\mu q_i^u\lambda_u R_u^2)\right]}{\pi\mu q_i^u\lambda_u\left(1-e^{-\pi\mu q_i^u\lambda_u R_u^2}\right)}\Bigg)\exp\Bigg(-\frac{(\tau-1)(\pi\mu q_i^u\lambda_u)^{-\frac{2}{\alpha}}\gamma\left(\frac{\alpha}{2}+1,\pi\mu q_i^u\lambda_u R_u^2\right)}{\rho_1\left(1-e^{-\pi\mu q_i^u\lambda_u R_u^2}\right)}\Bigg)$$
$$+(1-P_{f,i}^u)P_{f,i}^r \exp\left(-\frac{\beta\tau^{\frac{2}{\alpha}}\left[1-e^{-\pi q_i^r\lambda_r R_r^2}(1+\pi q_i^r\lambda_r R_r^2)\right]}{\pi q_i^r\lambda_r\left(1-e^{-\pi q_i^r\lambda_r R_r^2}\right)}\right)\exp\left(-\frac{(\tau-1)(\pi q_i^r\lambda_r)^{-\frac{2}{\alpha}}\gamma\left(\frac{\alpha}{2}+1,\pi q_i^r\lambda_r R_r^2\right)}{\rho_2\left(1-e^{-\pi q_i^r\lambda_r R_r^2}\right)}\right)\Bigg]. \quad (30)$$

From the analytical θ_i^{lb}, the lower bound T_s^{lb} is given by

$$T_s^{lb} = \sum_{i=1}^{N} f_i(\mu q_i^u + \theta_i^{lb}), \quad (31)$$

which contains the elementary functions only, and hence it is easily to be evaluated.

IV. Optimization of Secure Cache Placement

In this section, we aim to design the secure cache placement by maximizing the secure cache throughput. The optimization problem can be formulated as

$$\max_{\mathbf{q}^u,\mathbf{q}^r} T_s = \sum_{i=1}^{N} f_i\left\{\mu q_i^u + (1-\mu q_i^u)\right.$$
$$\times\left[\left(1-e^{-\pi\mu q_i^u\lambda_u R_u^2}\right)G(\mu q_i^u\lambda_u,\rho_1,R_u)\right.$$
$$\left.\left.+e^{-\pi\mu q_i^u\lambda_u R_u^2}\left(1-e^{-\pi q_i^r\lambda_r R_r^2}\right)G(q_i^r\lambda_r,\rho_2,R_r)\right]\right\}, \quad (32)$$

with constraints

$$\begin{cases} \sum_{i=1}^{N} q_i^u \le C_U, \\ \sum_{i=1}^{N} q_i^r \le C_R, \\ q_i^u \in [0,1], \quad i\in[1,N] \\ q_i^r \in [0,1], \quad i\in[1,N] \end{cases}, \quad (33)$$

where the caching parameters q_i^u and q_i^r should be optimized. In general, this optimization problem is non-convex, and it is difficult to obtain an analytical solution. Hence, we apply the heuristic algorithm to find the near-optimal solution, instead of deriving a closed-form solution. The details about the optimization of heuristic algorithm are shown in Algorithm 1.

In Algorithm 1, there are one main program and three functions of max_relay, max_user and GA. As the cache-enabled users follow the homogeneous PPP with density $\mu\lambda_u$ ($\mu \in [0,1]$), we need to consider two cases of $\mu = 0$ and $\mu > 0$. If $\mu = 0$ where none of users has cached the requested content, we only need to optimize the cache placement at relays; otherwise, the cache placement at both the relays and users should be studied. In this paper, we use the step-by-step optimization to solve the problem of optimizing the cache placement. As shown in line 5 of Algorithm 1, we first optimize the cache placement at relays to optimize the system performance on the relays, and then optimize the cache placement at the users, in order to maximize the secure cache throughput. The max_relay function is presented from line 7 to 15, and it returns the optimal cache probability $\mathbf{q}^r$. The max_user function is presented from line 16 to 24, and it uses $\mathbf{q}^r$ as a given condition into T_s, and then optimizes the cache placement at users to maximize the secure cache throughput. The GA function is the main function of the genetic algorithm (GA) [16], shown from line 25 to 33. The first step of GA function is to define the number of variables (line 26), the second step is to initialize the lower bound (LB) and upper bound (UB) of variables (line 27), the third step is to set the expression of fitness, and the fourth step is to set the constraint of fitness. Using the GA to find the optimal value is presented from line 30 to 33. As the GA function returns the minimum value, we define argument $fval$ as the negative of T_s, in order to find the maximum value of secure cache throughput.

V. Numerical Results and Discussions

In this section, we present some numerical results and discussions to verify the proposed studies, and illustrate the effect of key parameters on the secure cache throughput. We set the proportion of cache-enabled users μ to 0.8, and the radiuses of searching the requested content from the surrounding cache-enabled users and relays are set to 50m and 100m, respectively. The secrecy data rate R_s is set to 0.2 bps/Hz, and the noise variance is set to unity. We compare the proposed cache strategy with the conventional MPC and EPC cache strategies, in order to demonstrate the superiority of the proposed cache strategy.

Fig. 2 shows the secure cache throughput versus the number of file contents N, where $P_r = 30$dB, $P_u = P_r/5$, $\lambda_u = 2\times10^{-2}$, $\lambda_r = 4\times10^{-3}$, $\lambda_e = 1\times10^{-5}$, $C_U = 2$, $C_R = 5$, $\alpha = 2.1$ and $\gamma = 1.2$. As shown in this figure, the proposed cache strategy outperforms the conventional MPC and EPC cache strategies. This is because that MPC only exploits the signal cooperation gain, while EPC only achieves the content delivery gain. In contrast, the proposed cache strategy obtains a fine balance between the signal cooperation gain and the content delivery gain. Moreover, the secure cache throughput of the three cache strategies becomes worse with larger value of N, as more file contents lead to a smaller probability that the files are cached. In further, the proposed cache strategy deteriorates with N much slower than MPC and EPC, which also shows the superiority of the proposed cache strategy.

Fig. 3 illustrates the effect of the transmit power P_r on the secure cache throughput, where $N = 10$, $\lambda_u = 2\times10^{-2}$, $\lambda_r = 4\times10^{-3}$, $\lambda_e = 1\times10^{-5}$, $C_U = 2$, $C_R = 6$, $\alpha = 2.1$ and

Algorithm 1 Optimization of Secure Cache Placement

Input: Parameters N, λ_u, λ_r and λ_e

Output: Maximization of secure cache throughput $T_{s,max}$, the optimal caching probability $\mathbf{q}^r = [q_1^r, \ldots, q_N^r]$ and $\mathbf{q}^u = [q_1^u, \ldots, q_N^u]$.

if $\mu = 0$ **then**
  $\mathbf{q}^u = 0$
  $T_{s,max} = max\_relay(N, \lambda_r, \lambda_e)$
else
  $T_{s,max} = max\_user(max\_relay(N, \lambda_r, \lambda_e), \lambda_u)$
end if
function $max\_relay(N, \lambda_r, \lambda_e)$
  global $\mathbf{q}^r$
  $\mathbf{q}^u = 0$
  for $i = 1 : N$ **do**
    $[q_i^r, T_{s,max}^{relay}] = GA(N)$
    $\mathbf{q}^r(i) = q_i^r$
  end for
  return $[\mathbf{q}^r, T_{s,max}^{relay}]$
end function
function $max\_user(\mathbf{q}^r, \lambda_u)$
  global $\mathbf{q}^r$
  Use $\mathbf{q}^r$ as a known condition into T_s
  for $i = 1 : N$ **do**
    $[q_i^u, T_{s,max}] = GA(N)$
    $\mathbf{q}^u(i) = q_i^u$
  end for
  return $[\mathbf{q}^u, T_{s,max}]$
end function
function $GA(N)$
  $nvars = N$
  Initialize LB and UB of variables
  ObjectiveFunction=@$ga\_fitness$
  ConstraintFunction=@$ga\_constraint$
  $[q_i, fval] =$
   $ga(ObjectiveFunction, nvars,[],[],[],[],$
   $LB, UB, ...ConstraintFunction, options)$
  $max = -fval$
  return $[q_i, max]$
end function

$\gamma = 1.2$. From this figure, we can find that the secure cache throughput of three cache strategies improves with larger P_r, as higher transmit power can help enhance the transmission reliability and security. Moreover, the proposed cache strategy outperforms the MPC and EPC cache strategies for various values of transmit power. In particular, the EPC strategy improves much more rapidly than the other two strategies, and it even outperforms the MPC when the transmit power is very high. This is because that the probability of successful transmission of content becomes better as the transmit power increases, which improves the content delivery gain.

Fig. 4 depicts the impact of the cache size C_R and C_U on the secure cache throughput, where $N = 20$, $P_r = 30$ dB,

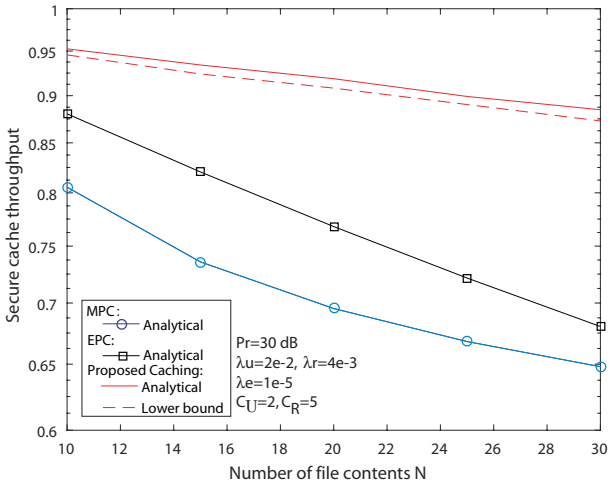

Fig. 2. Secure cache throughput versus the number of file contents N.

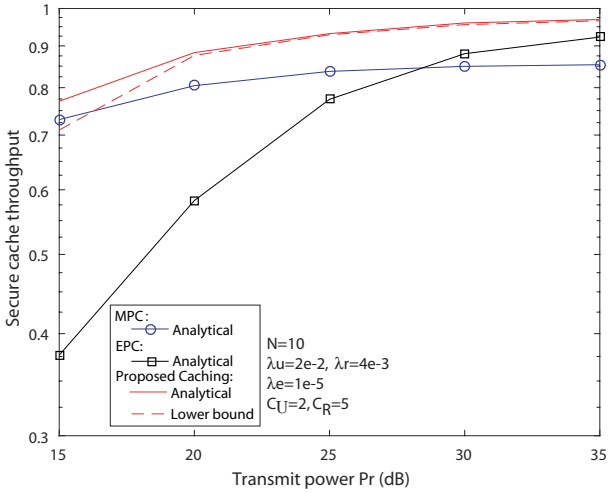

Fig. 3. Effect of the transmit power on the secure cache throughput.

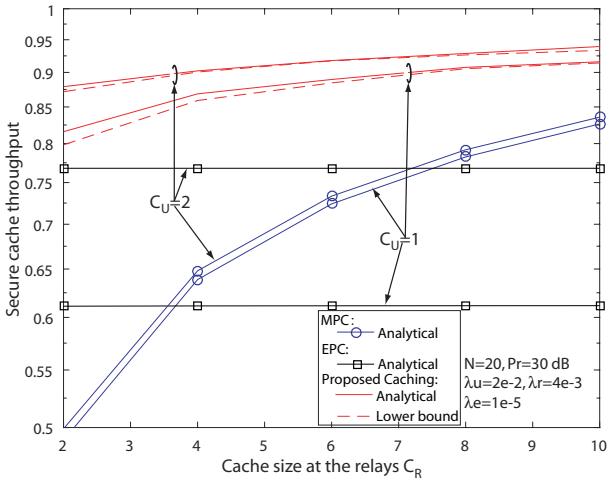

Fig. 4. Impact of C_R and C_U on the secure cache throughput.

$\lambda_u = 2 \times 10^{-2}$, $\lambda_r = 4 \times 10^{-3}$, $\lambda_e = 1 \times 10^{-5}$, $\alpha = 2.1$ and $\gamma = 1.2$. As observed from this figure, we can find that the proposed cache strategy outperforms the MPC and EPC cache strategies for various values of C_R and C_U, which further validates the effectiveness of the proposed caching strategy. Moreover, the secure cache throughput of the three caching strategies improves with increasing C_R, as larger cache size can help pre-store more file contents at the relay. In particular, EPC improves very limitedly with larger C_R, as the content delivery gain of EPC has already been saturated. In further, the lower bound of the proposed caching strategy become much closer to the exact value when C_R increases. Furthermore, the secure cache throughput of the proposed cache strategy, MPC and EPC cache strategies with $C_U = 2$ is larger than that with $C_U = 1$. This is because the content delivery gain increases with larger value of C_U, which improves the secure cache throughput.

VI. Conclusions

In this paper, we proposed a secure probabilistic caching strategy for the stochastic multi-user multi-relay networks in the presence of multiple eavesdroppers. We designed the secure caching placement at users and relays by taking into account several cache-aided transmission modes of self-fetch, D2D-transmission, relay-transmission, and the source-transmission. The network secrecy performance was studied by analyzing the secure cache throughput. To maximize the secure cache throughput, we optimized the probabilistic caching strategy by using the heuristic algorithm. Numerical results and discussion were provided to demonstrate the superiority of the proposed probabilistic caching strategy over the conventional MPC and EPC ones.

Appendices

A. Proof of Eq. (29)

According to (20), the function $G(\lambda, \rho, R)$ is rewrite as

$$G(\lambda,\rho,R) = \int_0^R \frac{2\pi\lambda r}{1-e^{-\pi\lambda R^2}} \exp\left(-\beta\tau^{\frac{2}{\alpha}} r^2\right) \times \exp\left(-\frac{\tau-1}{\rho} r^{\alpha}\right) e^{-\pi\lambda r^2} dr \quad \text{(A.1)}$$

$$= E_r\left[\exp\left(-\beta\tau^{\frac{2}{\alpha}} r^2\right)\right] E_r\left[\exp\left(-\frac{\tau-1}{\rho} r^{\alpha}\right)\right]. \quad \text{(A.2)}$$

According to Jensen inequality [15], we have

$$G(\lambda,\rho,R) \geq \exp\left(-\beta\tau^{\frac{2}{\alpha}} E_r\left[r^2\right]\right) \exp\left(-\frac{\tau-1}{\rho} E_r\left[r^{\alpha}\right]\right).$$

Based on the PDF of the distance in (17), we calculate $E_r\left[r^2\right]$ as

$$E_r\left[r^2\right] = \int_0^R r^2 \frac{2\pi\lambda r}{1-e^{-\pi\lambda R^2}} e^{-\pi\lambda r^2} dr = \frac{\pi\lambda}{1-e^{-\pi\lambda R^2}} \int_0^R r^2 e^{-\pi\lambda r^2} d\left(r^2\right) \overset{(b)}{=} \frac{1-e^{-\pi\lambda R^2}(1+\pi\lambda R^2)}{\pi\lambda\left(1-e^{-\pi\lambda R^2}\right)}, \quad \text{(A.3)}$$

where the step (b) uses the result of $\int_0^u x e^{-\mu x} dx = \frac{1}{\mu^2} - \frac{1}{\mu^2} e^{-\mu u}(1+\mu u)$. We further compute $E_r\left[r^{\alpha}\right]$ as

$$E_r\left[r^{\alpha}\right] = \int_0^R r^{\alpha} \frac{2\pi\lambda r}{1-e^{-\pi\lambda R^2}} e^{-\pi\lambda r^2} dr = \frac{\pi\lambda}{1-e^{-\pi\lambda R^2}} \int_0^R r^{\alpha} e^{-\pi\lambda r^2} d\left(r^2\right) \overset{(c)}{=} \frac{(\pi\lambda)^{-\frac{\alpha}{2}}}{1-e^{-\pi\lambda R^2}} \gamma\left(\frac{\alpha}{2}+1, \pi\lambda R^2\right), \quad \text{(A.4)}$$

where the step (c) holds due to the integral formula $\int_0^u x^n e^{-\mu x} d_x = \mu^{-n-1}\gamma(n+1, \mu u)$. By combining the results in (A.3) and (A.4), we obtain the lower bound of $G(\lambda, \rho, R)$ function, as shown in (29).

References

[1] M. A. M. Ali and U. Niesen, "Fundamental limits of caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 2856–2867, 2014.

[2] M. A. M. Ali and U. Niesen, "Coding for caching: Fundamental limits and practical challenges," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 23–29, 2016.

[3] M. M. Amiri and D. Gndz, "Fundamental limits of caching: Improved delivery rate-cache capacity trade-off," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 806–825, 2017.

[4] Z. Chen, J. Lee, T. Q. S. Quek, 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, 2017.

[5] G. Zheng, H. A. Suraweera, and I. Krikidis, "Optimization of hybrid cache placement for collaborative relaying," *IEEE Commun. Lett.*, vol. 21, no. 1, pp. 442–445, 2017.

[6] K. Li, C. Yang, Z. Chen, and M. Tao, "Optimization and analysis of probabilistic caching in n-tier heterogeneous networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1283–1297, 2018.

[7] D. Malak, M. Al-Shalash, and J. G. Andrews, "Spatially correlated content caching for device-to-device communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 56–70, 2018.

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

[9] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE Journal on Sel. Areas in Commun.*, vol. 36, no. 4, pp. 788–801, 2018.

[10] M. K. Kiskani, H. R. Sadjadpour, "A secure approach for caching contents in wireless Ad Hoc networks," *IEEE Trans. Vehic. Tech.*, vol. 66, no. 11, pp. 10249-10258, 2017.

[11] N. Zhao, F. Cheng, F. R. Yu, J. Tang, Y. Chen, G. Gui, and H. Sari, "Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 2281–2294, 2018.

[12] F. Shi, W. Tan, and et.al, "Hybrid cache placement for physical-layer security in cooperative networks," *IEEE Access*, vol. 6, pp. 8098–8108, 2018.

[13] D. Moltchanov, "Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146–1166, 2012.

[14] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal on Sel. Areas in Commun.*, vol. 27, no. 7, pp. 1029–1046, 2009.

[15] I. S. Gradshteuin, I. M. Ryzhik, A. Jeffrey, and D. Zwillinger, *Table of Integrals, Series, And Products*. Academic Press, 1980.

[16] J. R. Fernandez, J. A. Lpez-Campos, A. Segade, and J. A. Viln, "A genetic algorithm for the characterization of hyperelastic materials," *Applied Mathematics and Computation*, vol. 329, pp. 239–250, 2018.