Wireless Caching Helper System with Heterogeneous Traffic and Secrecy Constraints

Georgios Smpokos*†, Nikolaos Pappas†, Zheng Chen‡ and Parthajit Mohapatra§
*Network Evolution & Technology Planning, Vodafone, Greece
†Department of Science & Technology, Linköping University, Sweden
‡Department of Electrical Engineering, Linköping University, Sweden
§Department of Electrical Engineering, Indian Institute of Technology, Tirupati, India
Email: georgios.smpokos@vodafone.com, {nikolaos.pappas, zheng.chen}@liu.se, parthajit@iittp.ac.in

***Abstract*—In this paper we investigate and analyze the performance of a wireless system with caching capabilities while imposing secrecy constraints at one of the users. A dedicated user with secrecy constraints is always served by a helper/access point while a second user with no secrecy constraints receives content either from the helper or the core network through a macro cell base station. This non-dedicated user is served by the cellular network if it cannot find the requested content in the helper's cache. The presence of an eavesdropper trying to decode the content for the dedicated user affects the performance of the system in terms of average throughput and delay while allocated transmission power, request, and caching characteristics vary.**

I. Introduction

The upcoming wireless network evolution in 5G will not only enable upgrades in throughput, latency and scalability but additionally will enable higher levels of secure communications. Based on that, in the last decade physical layer secrecy has emerged as a promising approach over wireless networks as it exploits the inherent randomness present in the wireless channel to provide secure communication.

Nowadays, video content is the dominant type of wireless data traffic while videos can be stored proactively at the network edge nodes before being requested. Motivated by this, caching at the edge of the network has been identified as a promising approach to meet the high demand of the users in terms of rich content (e.g. video, image) [1]. The key idea is to store some likely-to-be-requested content at the network edge nodes according to some predefined caching policies (e.g. most popular content, random, coded) during off-peak hours [2]–[5]. When users request for some content that is already cached in the nearby nodes, the content delivery delay and energy consumption can be greatly reduced. While in wireless networks users have different secrecy requirements, it is important to analyze the impact of caching on the system performance under secrecy constraints and heterogeneous traffic conditions.

This work considers a network scenario with two users and an eavesdropper trying to overhear the transmissions from the helper to the dedicated user. The dedicated user with secrecy constraints does not request cacheable content but rather receives bursty traffic from the helper while the non-dedicated user without secrecy constraints requests reusable (cache-able) content that can be stored at edge node's (helper) cache. If the non-dedicated user requests some content that is not found at the helper's cache, then this user is served by a backhaul network server through a base station. When the helper needs to serve multiple users simultaneously, the decoding capability of the users can eventually affect the system's performance. Hence, it is important to explore how the concurrent transmission from the helper to different users can assist in providing secure communication under different decoding schemes at the users while an eavesdropper, which is not part of the network and is passive tries to listen to the communications of the helper node to the dedicated user.

This work has been supported in part by the Horizon 2020 Marie Skłodowska-Curie Actions project WiVi-2020 (H2020-MSCA-ITN-2014-EID 642743-WiVi-2020), and by ELLIIT and CENIIT.

A. Related Work

The result in [6] was a stepping stone for physical layer secrecy, where it was shown that it is possible to send messages securely over a noisy channel without using any key between the legitimate nodes. The problem of secure communication over multiuser scenarios has been studied extensively under different settings [7], [8], [10]–[12]. The impact of fading on secure communication has been explored under various settings in [9], [13]–[15]. It has been found that fading in wireless channel can facilitate secure communication in contrast to the case of Gaussian wiretap channel [13], [14].

In many real-world scenarios, data arrival at the access point nodes is random. Using queuing theory tools, the analysis for bursty traffic gives us a perspective that cannot be utilized with the assumption of saturated traffic [16]. In the existing literature, the impact of reliability and secrecy on the stability of the system is not well explored. In [17], the impact of reliability and security on the stability of the system is considered for the broadcast channel under different collaborative models for the eavesdroppers. In [18], the impact of secrecy constraint on the stability region of broadcast channel is explored under various decoding schemes at the users.

The study in [19] provided analysis on stable throughput and delay performance for single bottleneck cache enabled networks using stochastic request arrivals at different nodes. In [20], the authors investigated how bursty traffic and random caching availability of a small cell node affects the delay and

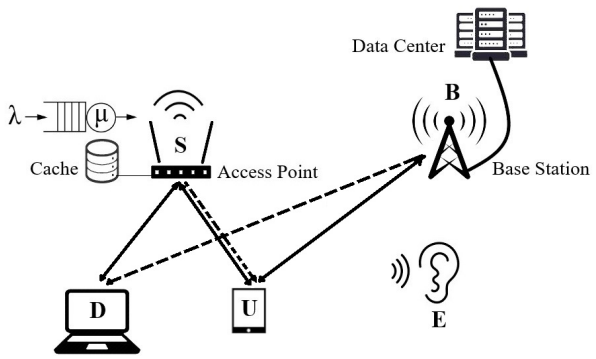

Fig. 1. System Model. D: dedicated user with secrecy requirements, U: user requesting cachable content with no secrecy requirements, E: Eavesdropper. Continuous and discontinued lines indicate possible active links and interference signals respectively.

throughput performance of a wireless caching system with two users although the secrecy of the communication is not taken into consideration.

B. Contribution

This work considers a simple network setup where two users with different secrecy and traffic characteristics, are served through a wireless helper system with caching capabilities. The helper node deploys superposition coding (SC) in order to allow simultaneous transmission to both users. Within the superposition coding scheme, the orthogonality for parallel transmission does not hold anymore and a non-orthogonal multiple access (NOMA) scheme is deployed. For this setup we obtain closed formulas for the average throughput and the average delay performance of the system analysing the impact of secrecy and caching in the numerical evaluation.

II. Network Model

The network considered as in Fig. 1 serves two users with different secrecy characteristics. The dedicated user D with secrecy requirements is only served by the helper/access point S. It is assumed that S always serves the arriving bursty traffic intended for the dedicated user D. The arrival process at S is characterized by the arrival rate λ. The helper S can additionally serve another user in parallel, namely the non-dedicated user U, that can request content initially from the helper's cache and if it cannot find it stored at S's cache it requests the content from a network cache (data center through the cellular network-base station B). Within this setup two users with different security requirements are served applying superposition coding [21] for the parallel transmissions to safeguard the transmission with security constraints (S to D).

Secrecy constraints arise due to the presence of an eavesdropper E in the vicinity of the helper S. E attempts to decode the content for the dedicated user D thus we intent to explore the randomness of the physical channel to establish secure connectivity between the helper S and D while there is parallel transmission to another user from either the helper S or the base station B. The total power transmitted by S is limited and the sum of power allocation for the parallel transmissions is always equal to the maximum transmit power level at S. In this setup both D and U as well as E treat interference as noise (TIN)[1].

In our scenario, the probability that helper S is available to serve the dedicated user D is denoted as q_S. The non-dedicated user U will request content outside its storage with probability q_U, that is equal to a miss probability trying to retrieve content from its own cache.

A. Caching Policy and Transmission Model

The probability that helper S can provide the requested content to U equals the hit probability p_h. The hit probability is related to the caching policy at the helper S and the request rates of content at U and S [2]. In the case of a miss with probability equal to $p_m = 1 - p_h$, the content needs to be delivered to U by the data center through the base station B. If the core network is available with a probability of α (lower values of α equal more congested network) then the content requested by the non dedicated user U will be sent through the base station and two parallel transmissions will take place if the helper S is available to serve D with probability q_S.

B. Physical Layer Model

In this setup a key parameter affecting the performance of the overall system is the transmission power allocation at the helper S P_S. We consider the transmission power level at S constant and equal to its maximum value P_{max} as the sum of power allocations P_{SD} and P_{SU} for the superposition coded transmission equals that value:

$$P_S = P_{SD} + P_{SU} = P_{max} \tag{1}$$

The transmission power level of the base station B is denoted as P_B and is dedicated to user U thus interfering with the S to D transmission. We assume this although it will cause interference to the dedicated user as it will additionally cause interference to the eavesdropper, eventually increasing the secrecy of the S to D communication.

In this work we consider Rayleigh fading channel characteristics and a power-law path loss model without any shadowing effects. Both users in order to successfully decode their content need to receive so that signal to noise plus interference ratio level (SINR) is higher than their demodulation threshold θ_j (θ_D, θ_U). In the case of a single transmission there is only signal to noise ratio (SNR) taken into consideration. For successful decoding the following expression needs to be satisfied for each receiver:

$$\text{SINR}_{ij/L} = \frac{P_{ij}|h_{ij}|^2 r_{ij}^{-\gamma}}{n_j + \sum_{k \in T \setminus \{i\}} P_{kj}|h_{kj}|^2 r_{kj}^{-\gamma}} \geq \theta_j \tag{2}$$

where in this scenario $i \in (S, B)$ and $j \in (D, U)$. In (2):

- L represents the set of active links (e.g. SD, SU, BU)

[1]The case where the receivers can apply successive decoding will be studied in an extension of this work due to space limitation.

[2]For a detailed treatment regarding hit/miss probability and the cache size please refer to [20].

- T is the set of active transmitters (S, B).
- P_{ij} is the power from transmitter i to receiver j.
- h_{ij} is the Rayleigh fading cannel component with $\mathcal{CN}(0,1)$.
- r_{ij} is the distance between transmitter i and the receiver j.
- n_j is the noise (AWGN) component at the receiver j.

The successful decoding of the intended content by each receiver will be denoted as the event $\mathcal{D}_{ij/L}$ where ij indicates the transmitter receiver pair and L all the active links. The event with secrecy constraints (e.g. S transmitting to D) will be denoted as $\mathcal{D}^{\star}_{ij/L}$. The transmitter-receiver pairs characterize the events of the form:

$$\mathcal{D}^{\star}_{ij/L} = \left\{ \text{SINR}_{ij/L} \geq \theta_j, \text{SINR}_{iE/L} < \theta_j \right\} \tag{3}$$

with secrecy constraints (second term at (3) the SINR at the eavesdropper E) and

$$\mathcal{D}_{ij/L} = \left\{ \text{SINR}_{ij/L} \geq \theta_j \right\} \tag{4}$$

with no secrecy constraints. The success probabilities $\mathcal{P}(\mathcal{D}^{\star}_{ij/L})$ and $\mathcal{P}(\mathcal{D}_{ij/L})$ (with and without secrecy constraints) of these events will be studied regarding their effect on the overall performance of the system. The expressions for the success probabilities can be obtained similarly with [18] and [21].

III. Throughput and Delay Analysis

In this section we provide the throughput and delay analysis for the considered system.

A. Throughput

The following throughput analysis characterizes the system illustrated in Fig. 1 and includes the outcome of the physical layer analysis. First, we will generate the expression of the average throughput of the dedicated user D that is characterized by the average service rate μ of the helper S and will be:

$$\begin{aligned} \mu = {} & q_S(1-q_U)\mathcal{P}(\mathcal{D}^{\star}_{SD/SD}) \\ & + q_S q_U p_h \mathcal{P}(\mathcal{D}^{\star}_{SD/SD,SU}) \\ & + q_S q_U p_m \alpha \mathcal{P}(\mathcal{D}^{\star}_{SD/SD,BU}) \\ & + q_S q_U p_m (1-\alpha)\mathcal{P}(\mathcal{D}^{\star}_{SD/SD}). \end{aligned} \tag{5}$$

In the case when the helper's S queue is stable the probability that the queue of size Q is not empty is given as follows:

$$\mathcal{P}(Q \neq 0) = \frac{\lambda}{\mu} \tag{6}$$

where μ is given by (5).

Next, we will express the average achieved throughput for the non-dedicated user U in the case where the queue at the helper S is not empty ($Q \neq 0$):

$$\begin{aligned} T_U = {} & q_S \mathcal{P}(Q \neq 0) q_U p_h \mathcal{P}(\mathcal{D}_{SU/SD,SU}) \\ & + q_S \mathcal{P}(Q \neq 0) q_U (1-p_h) \alpha \mathcal{P}(\mathcal{D}_{BU/SD,BU}) \\ & + [1 - q_S \mathcal{P}(Q \neq 0)] q_U p_h \mathcal{P}(\mathcal{D}_{SU/SU}) \\ & + [1 - q_S \mathcal{P}(Q \neq 0)] q_U (1-p_h) \alpha \mathcal{P}(\mathcal{D}_{BU/BU}). \end{aligned} \tag{7}$$

B. Delay

The average delay experienced by user U is illustrated in this section (average delay experienced by the dedicated user D is zero as it is served whenever S is available). Let us denote the average delay of user U as D_U.

$$\begin{aligned} D_U = {} & p_h q_s \mathcal{P}(Q \neq 0)\mathcal{P}(\mathcal{D}_{SU/SD,SU}) \\ & + p_h[1 - q_s \mathcal{P}(Q \neq 0)]\mathcal{P}(\mathcal{D}_{SU/SU}) \\ & + p_h q_s \mathcal{P}(Q \neq 0)[1 - \mathcal{P}(\mathcal{D}_{SU/SD,SU})](1 + D_S) \\ & + p_h[1 - q_s \mathcal{P}(Q \neq 0)][1 - \mathcal{P}(\mathcal{D}_{SU/SU})](1 + D_S) \\ & + p_m q_s \mathcal{P}(Q \neq 0)\alpha \mathcal{P}(\mathcal{D}_{BU/SD,BU}) \\ & + p_m[1 - q_s \mathcal{P}(Q \neq 0)]\alpha \mathcal{P}(\mathcal{D}_{BU/BU}) \\ & + p_m q_s \mathcal{P}(Q \neq 0)[1 - \alpha \mathcal{P}(\mathcal{D}_{BU/SD,BU})](1 + D_B) \\ & + p_m[1 - q_s \mathcal{P}(Q \neq 0)][1 - \alpha \mathcal{P}(\mathcal{D}_{BU/BU})](1 + D_B) \end{aligned} \tag{8}$$

where D_S and D_B are the average delay imposed by the helper S and the base station B respectively and are derived from the following expressions:

$$D_S = \frac{1}{q_s \mathcal{P}(Q \neq 0)\mathcal{P}(\mathcal{D}_{SU/SD,SU}) + [1 - q_s \mathcal{P}(Q \neq 0)]\mathcal{P}(\mathcal{D}_{SU/SU})} \tag{9}$$

$$D_B = \frac{1}{q_s \mathcal{P}(Q \neq 0)\alpha \mathcal{P}(\mathcal{D}_{BU/SD,BU}) + [1 - q_s \mathcal{P}(Q \neq 0)]\alpha \mathcal{P}(\mathcal{D}_{BU/BU})} \tag{10}$$

IV. Numerical Results

In this section we will include some results regarding the average throughput and delay for the non-dedicated user U for the cases when some of the characteristics of the system (power allocation, caching capabilities, hit rate) vary in the presence of an eavesdropper. In our analysis we assume that the noise variance is $\mathbb{E}[n_j^2] = 1$ and path-loss exponents $\gamma_S = 2$ for all of the paths from the helper S ($S \rightarrow D$, $S \rightarrow U$, $S \rightarrow E$) and $\gamma_B = 4$ for all of the paths from the base station B ($B \rightarrow D$, $B \rightarrow U$, $B \rightarrow E$). Transmission power levels at the helper S are $P_S = P_{SD} + P_{SU} = 1000$ and $P_B = P_{BU}$ is the transmission power of the base station. We will assume that both D and U are located at a specific distance from the helper S such that $r_{SD} = 10m$ and $r_{SU} = 20m$. The eavesdropper is located further such that $r_{SE} = 30m$. The distance of the dedicated and non-dedicated user as well as that of the eavesdropper from the base station B will be set to $1000m$ ($r_{BD} = r_{BU} = r_{BE} = 1000m$).

In Figures 2 and 3 we get the average throughput and delay for user U with and without secrecy constraints for different values of transmission power allocation at the helper S (normalized to P_{max}). The results for the scenario without secrecy constraints have been obtained by treating all events as in expression (4), where there is no eavesdropper present. As expected, the average delay without secrecy constraints is lower than that with secrecy constraints and average throughput is higher. As the power level of the transmission to the dedicated user D increases both throughput and delay performance deteriorate due to the higher interference caused

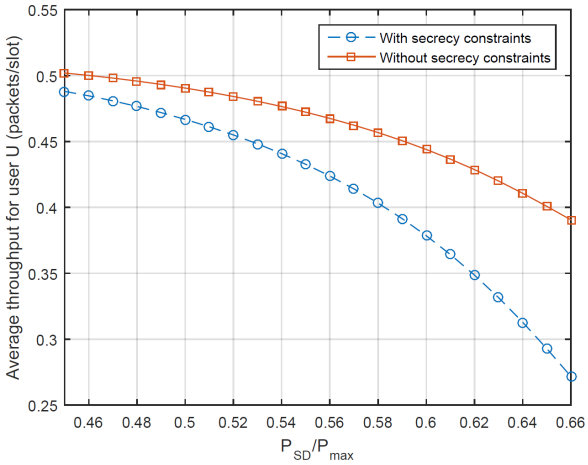

Fig. 2. Average throughput for user U T_U with and without secrecy constraints versus transmission power from helper S to the dedicated user D (normalized). The plot was generated with: $\lambda = 0.4$, $q_S = 0.9$, $q_U = 0.8$, $p_h = 0.6$, $\alpha = 0.7$, $\theta_D = 0.5$ and $\theta_U = 0.4$.

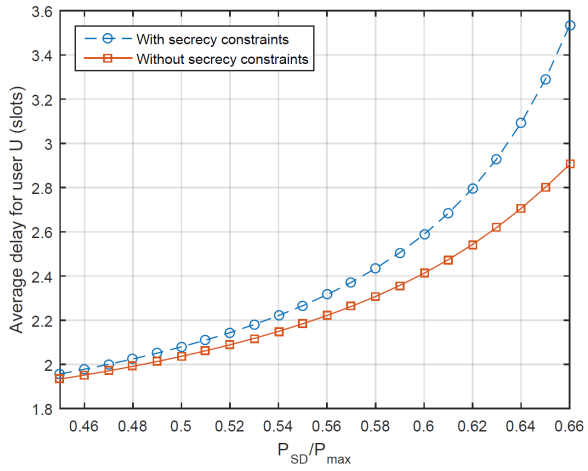

Fig. 3. Average delay for user U D_U with and without secrecy constraints versus transmission power from helper S to the dedicated user D (normalized). The plot was generated with: $\lambda = 0.4$, $q_S = 0.9$, $q_U = 0.8$, $p_h = 0.6$, $\alpha = 0.7$, $\theta_D = 0.5$ and $\theta_U = 0.4$.

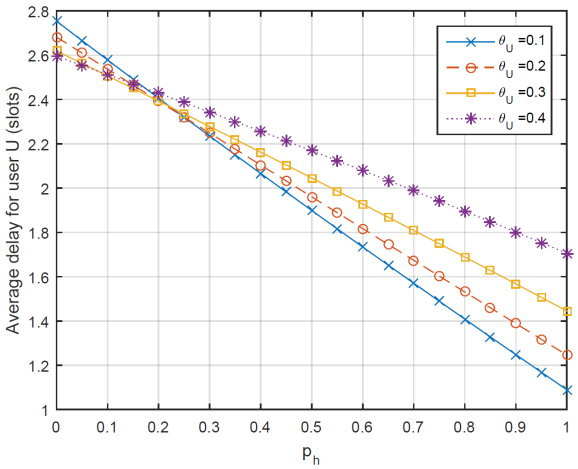

Fig. 4. Average delay for user U D_U for different values of demodulation threshold at U θ_U versus the hit rate at helper S p_h. The plot was generated with: $\lambda = 0.4$, $q_S = 0.9$, $q_U = 0.8$, $\alpha = 0.7$, $\theta_D = 0.5$ and $P_{SD} = P_{SU} = P_{max}/2$.

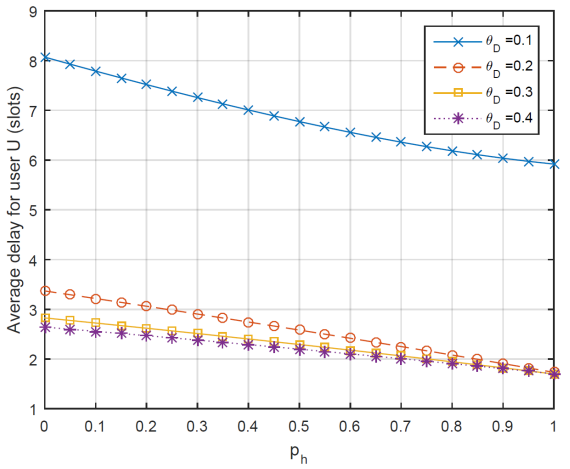

Fig. 5. Average delay for user U D_U for different values of demodulation threshold at D θ_U versus the hit rate at helper S p_h. The plot was generated with: $\lambda = 0.4$, $q_S = 0.9$, $q_U = 0.8$, $\alpha = 0.7$, $\theta_U = 0.4$ and $P_{SD} = P_{SU} = P_{max}/2$.

to U for both cases. It is notable that for lower values of power transmitted to the dedicated user D (P_{SD}) the performance of the system with secrecy constraints gets closer to that without any secrecy constraints.

In both Figures 4 and 5 we observe the average delay for user U versus the hit rate at helper S (p_h) for different values of demodulation threshold at U and D (θ_U, θ_D). For higher hit rate p_h at S (high probability to find the requested content at S's cache) we get lower delay for lower threshold values for user U (θ_U). For lower hit rate values (i.e. < 0.2) we get lower delay for higher threshold values at U. For lower hit rate values of the requested content from helper's cache it is better for U to try to find the content at the network's server thus receiving from B. In Fig. 5 we vary the threshold at the dedicated user D (θ_D) and as the hit rate increases the delay decreases while for higher values of θ_D the delay is lower due to increased secrecy.

Fig. 6 demonstrates the average delay performance for user U versus the probability of U requesting content outside its cache (content not found at U's cache) with and without secrecy constraints. It is notable that although the performance for all of q_U values is worse with secrecy constraints when applying secrecy, the delay decreases for higher values of request probability. The system behaves better in terms of delay for U when the user U requests content from the helper with higher probability. Finally, in Fig. 7 we can observe the average delay for user U versus the power allocated at the helper S when we vary the request probability at U q_U. As

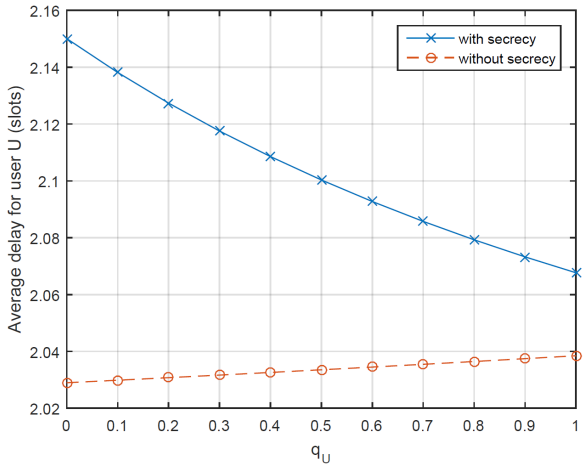

Fig. 6. Average delay for user U D_U with and without secrecy constraints versus the request probability q_U. The plot was generated with: $\lambda = 0.4$, $q_S = 0.9$, $p_h = 0.6$, $\alpha = 0.7$, $\theta_U = 0.4$, $\theta_D = 0.5$ and $P_{SD} = P_{SU} = P_{max}/2$.

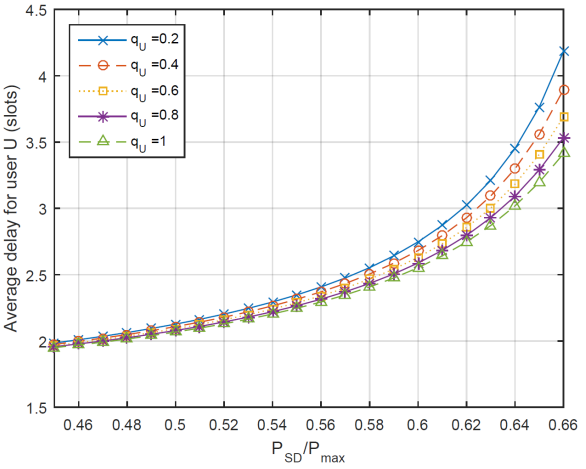

Fig. 7. Average delay for user U D_U versus transmission power from helper S to the dedicated user D (normalized) for different values of request probability at U q_U. The plot was generated with: $\lambda = 0.4$, $q_S = 0.9$, $p_h = 0.6$, $\alpha = 0.7$, $\theta_D = 0.5$ and $\theta_U = 0.4$.

indicated before we get better performance when there is high probability that U requests content from helper's S cache that can be observed for higher values of transmitted power for the S to D link (for low transmission power levels for S to U link). It is important to note that for low power levels for the S to D link (high power levels for S to U link) the performance is not significantly different for the different values of the request probability q_U thus making the system tolerant to big changes in the request probabilities from U.

V. Conclusions

The analysis we have presented so far provided an overview of performance under secrecy constraints, for the system considered. The availability of both the wireless helper (small cell) with caching capabilities and that of the base station were used in closed forms for both the average throughput and the delay. The system's performance in the presence of an eavesdropper deteriorates in terms of average throughput while the request and caching characteristics could compensate that performance degradation.

References

[1] E. Bastug, M. Bennis, and M. Debbah, "Living on the edge: The role of proactive caching in 5g wireless networks," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 82–89, Aug. 2014.

[2] N. Golrezaei, A. G. Dimakis and A. F. Molisch, "Scaling Behavior for Device-to-Device Communications With Distributed Caching," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4286-4298, July 2014.

[3] N. Golrezaei, K. Shanmugam, A. G. Dimakis, A. F. Molisch, and G. Caire, "Femtocaching: Wireless content delivery through distributed caching helpers," *Proc. IEEE INFOCOM*, pp. 1107-1115, Mar. 2012.

[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, May 2017.

[5] Z. Chen, N. Pappas and M. Kountouris, "Probabilistic Caching in Wireless D2D Networks: Cache Hit Optimal Versus Throughput Optimal," *IEEE Commun. Letters*, vol. 21, no. 3, pp. 584-587, March 2017.

[6] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1334-1387, Oct. 1975.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[8] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137-155, Jan. 2011.

[9] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453-2469, Jun. 2008.

[10] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2507, Jun. 2008.

[11] O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 5682-5694, Sept. 2011.

[12] E. Ekrem and S. Ulukus, "Effects of cooperation on the secrecy of multiple access channels with generalized feedback," *CISS*, Mar. 2008.

[13] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *Proc. IEEE Int. Symp. Inf. Theory*, pp. 356-360, Jul. 2006.

[14] P. K. Gopala, L. Lai and H. El Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[15] K. Jiang, T. Jing, Z. Li, Y. Huo and F. Zhang, "Analysis of secrecy performance in fading multiple access wiretap channel with SIC receiver," *IEEE INFOCOM*, May 2017.

[16] A. Ephremides and B. Hajek, "Information theory and communication networks: An unconsummated union," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2416-2434, Oct. 1998.

[17] Y. Liang, H. V. Poor, and L. Ying, "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 682-692, Sept. 2011.

[18] P. Mohapatra, N. Pappas, J. Lee, T. Q. S. Quek, V. Angelakis, "Secure communications for the two-user broadcast channel with random traffic," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, Sept. 2018.

[19] F. Rezaei and B. H. Khalaj, "Stability, rate, and delay analysis of single bottleneck caching networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 300-313, Jan. 2016.

[20] N. Pappas, Z. Chen and I. Dimitriou, "Throughput and delay analysis of wireless caching helper systems with random availability," *IEEE Access*, vol. 6, pp. 9667-9678, 2018.

[21] N. Pappas, M. Kountouris, A. Ephremides, V. Angelakis, "Stable throughput region of the two-user broadcast channel," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4611-4621, Oct. 2018.