The Asymptotic Secrecy Rate of Decentralized Wireless Networks

Hourieh Ghorbani
Faculty of Engineering
Shahed University
Tehran, Iran
Email: h.ghorbani@shahed.ac.ir

Soroush Akhlaghi
Faculty of Engineering
Shahed University
Tehran, Iran
Email: Akhlaghi@shahed.ac.ir

Sayed Ali Khodam Hoseini
Faculty of Engineering
Shahed University
Tehran, Iran
Email: khodamhoseini@shahed.ac.ir

Abstract— **This paper studies the achievable secrecy rate of a decentralized wireless network consisting of N communication links exchanging information over a shared channel. It is assumed that there are M eavesdroppers attempting to listen to the transmitted information. In this regard, an on-off strategy is proposed to maximize the achievable secrecy rate of such network. Accordingly, it is shown that for large values of N, when the number of eavesdroppers (M) is less than $\frac{N}{(\log n)^2}$, the achievable sum secrecy-rate scales as $\log\frac{2N}{M} - 2\log\log N + \frac{O_N(\log(N).\log\log(N))}{(\log N)^2}$.**

Keywords-component; assymptotic; decentralized network; secrecy-rate; eavesdropper;

I. INTRODUCTION

In recent years, tremendous data exchange through the wireless networks has encouraged service providers to incorporate some transmission protocols that utilize a shared medium to serve a large number of users. More recently, Ad-hoc networks have attracted much attentions to be utilized in such mediums, as any node of network may attempt to send information to any randomly chosen node of network via some intermediate nodes through using a multi-hop transmission strategy [1].

In this regard, there exists a number of works that have focused on the asymptotic behavior of ad hoc networks where the impact of fading and path loss are taken into account [1]-[3]. For instance, the capacity scaling of an ad-hoc network in the presence of additive Gaussian noise and path loss, is considered in [1]. Following by that, it is shown that the mobility factor increases the per user throughput of the network in [2], where the concept is thoroughly investigated in [3] under a general fading model.

On the other hand, using a shared medium between a large number of users has raised some privacy and secrecy challenges to protect information against eavesdropping. In this regard, providing a secure communication mechanism which guarantees the users' privacy, is an attractive option to deal with. Accordingly, a considerable number of works are devoted to explore the achievable secrecy rate of ad hoc networks under various conditions [4]-[8].

In a parallel path, the capacity scaling throughput has been investigated for isotropic single-hop channels. In [9], a network consisting of N transmitter-receiver pairs is studied, where it is assumed that each link can either transmit with a constant power or remain in silence. In this regard, the upper and the lower bounds on the network's capacity is derived in a Rayleigh fading environment. Some similar attempts have been made through [10]-[12]. In [10], the scaling behavior of the network's throughput is derived under the log-normal fading. Maximizing the number of active links is considered in [11], and the best link activation is considered for a general fading model in [12].

However, to the best of the authors' knowledge, the secrecy capacity of single-hop networks with asymptotically large number of legitimate and illegitimate users has not been addressed yet. We assume N disjoint communication links attempting to exchange information over a shared quasi-static isotropic block fading environment in which direct and cross channel gains are drawn from an i.i.d. complex Gaussian distribution of unit power. It is assumed that each transmitter has the Channel State Information (CSI) associated with its direct channel strength to its corresponding receiver.

Moreover, there are M eavesdroppers that are trying to decode the exchanged information between the legitimate pairs. It is assumed that the number of legitimate transmitter-receiver pairs is greater than that of the eavesdroppers. The channel between each transmitter and any unintended receiver is suffering from block fading and additive white Gaussian noise. The information transmission by any node in the described network causes some amount of interference at any unintended legitimate receiver. Thus, information transmission by all of the transmitters does not necessarily improve the overall secrecy rate of the network. In this case, an on-off transmission strategy, based on some predetermined threshold is devised. According to the proposed strategy, only the transmitters that have improving effect on the overall secrecy rate of the network are activated. In this regard, the optimum value of the activation threshold, the maximum number of eavesdroppers to have a non-vanishing secrecy rate, and the maximum achievable secrecy rate of the network are derived in a high interference region.

IEEE 2017© $31.00/978-1-5090-5963-8/17

Notation- In the current paper we will use bold capital letters and lower case bold letters to denote matrices and vectors, respectively. $\log(.)$ is the natural logarithm function; for functions $f(N)$ and $g(N)$ we denote $f(N) = o(g(N))$ if $\lim_{N\to\infty} \left|\frac{f(N)}{g(N)}\right| = 0$, $f(N) = O(g(N))$ if $\lim_{N\to\infty} \left|\frac{f(N)}{g(N)}\right| < \infty$ and $f(N) = \omega(g(N))$ if $\lim_{N\to\infty} \left|\frac{f(N)}{g(N)}\right| = \infty$. The event E_N is called asymptotically almost surely (a.a.s), if $Pr(E_N) \to 1$, when $N \to \infty$.

The rest of this paper is organized as follows. The system model, regarding the channel fading and noise characteristics are provided in Section II. Moreover, the main problem is introduced at the end of this section. The problem statement and the analytical solution is presented in Section III, and the simulation results are presented in Section IV. Finally, Section V concludes the paper.

II. System Model

A decentralized wireless communication network with N legitimate transmitter-receiver pairs and M non-cooperative illegitimate receivers, namely eavesdroppers, is considered. Each transmitter, e.g., the i'th one, can transmit its desired information to its corresponding receiver with a constant pre-determined power or remain silent (Fig. 1).

In this model, the set of active links is denoted by Λ and the objective is to maximize the sum secrecy capacity over the selection of active links in every time slot. The desired link selection policy is based on some channel strength threshold comparison, i.e., if the direct channel strength associated with a certain transmitter-receiver pair exceeds the threshold, the transmitter is activated. Assuming there are K active links among the available N transmit-receive nodes in one time-slot and resorting them from 1 to K, the received signal at the i'th receiver when its corresponding transmitter is active, can be represented by summation of the signals associated with the direct link and cross links, as follows,

$$y_i = h_{ii}x_i + \sum_{j=1, j\neq i}^{K} h_{ij}x_j + z_i, \qquad i = 1,2,...,K \tag{1}$$

In (1), h_{ij} represents the channel fading coefficient between the j'th transmitter and i'th receiver with channel strength $|h_{ij}|^2 = \gamma_{ij}$. As mentioned earlier, the network is under block fading, which means that h_{ij} is assumed to be fixed during one time-slot and varies independently for the upcoming time-slots. Moreover, x_i is the signal transmitted by the i'th transmitter from a complex Gaussian codebook with a zero mean and unit power, i.e., $E|x_i|^2 = 1$ and z_i is a complex circularly symmetric additive white Gaussian noise with unit variance. Moreover, there are M eavesdroppers in the network and the i'th one receives the transmitted signal associated with K active transmitters as follows,

$$y_l^e = \sum_{j=1}^{K} h_{lj}^e x_j + z_l^e, \qquad l = 1,2,...,M \tag{2}$$

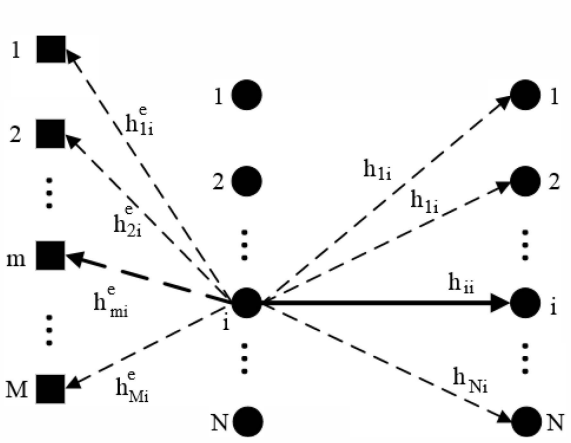

Figure 1. Considered comminiucation network. (figure caption)

In (2), h_{lj}^e denotes the channel coefficient between the l'th eavesdropper and the j'th transmitter where the corresponding channel strength is denoted by $|h_{lj}^e|^2 = \gamma_{lj}^e$. x_j represents the transmitted signal associated with the j'th active transmitter and z_i^e denotes the additive white complex Gaussian noise, i.e., $\mathcal{CN}(0,1)$ at the l'th eavesdropper. It is worth mentioning that the channel coefficient associated with the legitimate and illegitimate receivers, i.e., h_{ij} and h_{lj}, are assumed to follow a Gaussian distribution, which results in having an exponential distribution for their corresponding channel strengths.

In this regard, providing secrecy for i'th transmitter in physical layer, corresponds to communicating with a rate that the illegitimate receiver with the strongest channel strength cannot decode anything. In other words, considering $\{\gamma_{1i}^e, \gamma_{2i}^e, \dots, \gamma_{Mi}^e\}$ as the channel strengths between the i'th transmitter and the illegitimate receivers, the transmission policy depends on the maximum channel strength between the i'th transmitter and eavesdroppers, i.e., $\gamma_{\mathrm{m}i}^e = \max\{\gamma_{1i}^e, \gamma_{2i}^e, \dots, \gamma_{Mi}^e\}$. Thus, the secrecy capacity associated with the i'th receiver can be formulated as follows,

$$C_{i_{\mathrm{sec}}} = \left[\log(1+\frac{\gamma_{ii}}{1+I_i}) - \log(1+\frac{\gamma_{mi}^e}{1+I_i^e})\right]^{\dagger} \tag{3}$$

Where $[x]^{\dagger} = \max(x, 0)$. The first term in the right-hand side of (3) denotes the capacity of the i'th forward link and the second term denotes the capacity of the link between the i'th transmitter and its corresponding strongest eavesdropper. The term $I_i = \sum_{j=1, j\neq i}^{K} \gamma_{ij}$ denotes the interference power at the i'th receiver, which is caused by other active transmitters. Similarly, $I_i^e = \sum_{j=1, j\neq i}^{K} \gamma_{ij}^e$ plays the role of interference for the eavesdropper that enjoys the strongest channel strength to decode the i'th transmitter's information. Consequently, the sum secrecy capacity of the network can be defined as the summation of secrecy capacities, associated with all of the active transmitters as follows,

$$C_{\mathrm{scc}}^{sum} = \sum_{i=1}^{K} C_{i_{\mathrm{sec}}}. \tag{4}$$

In this paper, we are going to derive a lower bound on the sum secrecy capacity of the network (C_{sec}^{sum}), namely sum secrecy rate (R_{sec}^{sum}) and maximize the aforementioned rate by proposing the prescribed ON/OFF scheme.

III. MAXIMIZING THE SUM SECRECY RATE

In order to characterize the system performance, one can consider deriving a lower bound on the sum secrecy capacity of the network. We consider an ON/OFF scheme which activates a transmitter in the case that its direct signal to noise plus interference ratio (SINR) is above a certain threshold. We assume that a large number of active links are present in each transmission block, and according to the weak law of large numbers, the interference term tends to its mean value. Thus, the SINR consideration simplifies to the case of considering direct channel strength and activating a transmitter that has a direct channel strength greater than a predetermined threshold, i.e.,$\gamma_{ii} > t$. The validity of the aforementioned assumption on the number of active links, will be verified at the end of this section. In this case, the following inequalities can be written,

$$C_{\text{sec}}^{sum} > \sum_{i=1}^{K}(\log(1+\frac{t}{1+I_i})-\log(1+\frac{\gamma_{mi}^{e}}{1+I_i^{e}}))$$
$$\overset{(a)}{\geq} K\log(1+\frac{t}{1+\frac{1}{K}\sum_{i=1}^{K}I_i})-\sum_{i=1}^{K}\log(1+\frac{\gamma_{\text{m}i}^{e}}{1+I_i^{e}}), \quad (5)$$

Where (a) in (5) is obtained by incorporating the Jensen's inequality [13]. To characterize the system performance, one can consider that the strongest channel strength between any transmitter and eavesdroppers is lower than a certain value, with unit probability. For the case of complex zero-mean and unit-variance Gaussian channel coefficient between the i 'th eavesdropper and the j 'th transmitter, i.e., h_{ij}^{e}, the channel strength, i.e., γ_{ij}^{e}, follows an exponential distribution with unit mean and variance. Thus, it can be easily shown that the maximum channel strength associated with the i'th transmitter has the following cumulative distribution function (CDF),

$$F_{\gamma_{mi}^{e}}(y)=\Pr(\gamma_{\text{m}i}^{e}<y)=(1-e^{-y})^{M-1} \quad (6)$$

Noting the fact that the communication is occurred in the presence of a large number of eavesdroppers, we try to find a threshold that slightly deviating from it in positive values results in tending $F_{\gamma_{mi}}$ to unity, and slightly deviating from it to the negative values, results in tending the aforementioned CDF to zero in an a.a.s sense. In this regard, using some simple mathematics, one can arrive at $y=\log M$ as the maximizer point of the associated pdf. Noting the following limitations,

$$\lim_{M\to\infty}\Pr\left(\gamma_{mi}^{e}\leq\log M-\lambda\right)=\lim_{\text{M}\to\infty}\left(1-\frac{e^{\lambda}}{M}\right)^{M}$$
$$=e^{-e^{\lambda}}=o_M\left(\frac{1}{e^{M}}\right), \quad (7)$$

$$\lim_{M\to\infty}\Pr\left(\gamma_{mi}^{e}\leq\log M+\lambda\right)=\lim_{M\to\infty}\left(1-\frac{e^{-\lambda}}{M}\right)^{M}=e^{-e^{-\lambda}}$$
$$=e^{-e^{-o_{\text{M}}(\log M)}}=e^{-o_M\left(\frac{1}{M}\right)}=1-o_M\left(\frac{1}{M}\right), \quad (8)$$

it can be turned out that one can consider the maximum channel strength associated with the eavesdroppers as $\Delta=\log M+\lambda$, where $\lambda=\omega(1)=o_M(\log M)$. Thus, one can replace the maximum channel strength between the i 'th transmitter and the eavesdroppers with Δ, in (6). Moreover, since the channel coefficients, i.e., h_{ij}s are complex Gaussian random variables of zero mean and unit variance, the channel strengths, i.e., γ_{ij} s are exponentially distributed with unit mean and variance. Since, the interference terms I_i and I_i^{e} are the sum of the$K-1$ random variables with exponential distribution, they are Gamma distributed with mean and the variance equal to $K-1$. As a result, incorporating the Chebyshev inequality for some real and positive value of $\xi=\omega(1)$, the lower and upper bounds of the interference terms can be formulated as follows,

$$K-1-\xi\sqrt{K-1}<I_i<K-1+\xi\sqrt{K-1} \quad (9)$$

One can take an average of (9) on all of the values of i $(1\leq i\leq K)$ and write the following relation,

$$K-1-\xi\sqrt{K-1}<\frac{1}{K}\sum_{i=1}^{K}I_i<K-1+\xi\sqrt{K-1} \quad (10)$$

Defining$\psi\triangleq\xi\sqrt{K-1}=\omega(1)$ that satisfies$\psi=o_K(K)$, the lower bound of (5) can be written as follows,

$$R_{\text{sec}}^{sum}\geq K\log(1+\frac{t}{K+\psi})-K\log(1+\frac{\Delta}{K-\psi}). \quad (11)$$

Additionally, due to the on-off behavior of the active links, K is a binomial random variable with parameters N and q, where considering the $F_{\Gamma_{ii}}(\gamma_{ii})$ as the (CDF) of the direct channel strength between the i'th transmitter and receiver pair, $q=1-F_{\Gamma_{ii}}(\gamma_{ii})$ denotes the probability of the link activation. Consequently, considering t as the activation threshold, one would arrive at $q=e^{-t}$. Again, incorporating the Chebyshev inequality the lower and upper bounds on the number of the active link are obtained as follows,

$$Nq-\nu\sqrt{Nq}<K<Nq+\nu\sqrt{Nq} \quad (12)$$

Where $\nu=\omega(1)$. Knowing that (11) is an increasing function with respect to K, one would substitute the parameter with its lower bound and write,

$$R_{\text{sec}}^{sum}\geq(Nq-\nu\sqrt{Nq})\log(1+\frac{t}{(Nq-\nu\sqrt{Nq})+\psi})$$
$$-(Nq-\nu\sqrt{Nq})\log(1+\frac{\Delta}{(Nq-\nu\sqrt{Nq})-\psi}). \quad (13)$$

In what follows, we tend to find the optimum threshold of the link activation. Considering $\psi=o_K(K)$, it can be neglected

from the denumerator of the SINR terms, as comparing it with K. Therefore, the equation (13) can be simplified to,

$$R_{\text{sec}}^{sum} = (Ne^{-t} - \nu\sqrt{Ne^{-t}})\log(1+\frac{t}{(Ne^{-t} - \nu\sqrt{Ne^{-t}})}) - (Ne^{-t} - \nu\sqrt{Ne^{-t}})\log(1+\frac{\Delta}{(Ne^{-t} - \nu\sqrt{Ne^{-t}})}). \quad (14)$$

To get a starting point for the threshold value, we temporarily forget the term $\nu\sqrt{Ne^{-t}}$ in (14) and write the equation in the following form,

$$R_{\text{sec}}^{sum} = Ne^{-t}\log(1+\frac{t}{Ne^{-t}}) - Ne^{-t}\log(1+\frac{\Delta}{Ne^{-t}}) \quad (15)$$

The result of (15) will help us in finding the actual optimum value of activation threshold. Taking the approximation of $\log(1+x) \approx x - \frac{x^2}{2}$ into account, the achievable secrecy rate can be formulated as follows,

$$R_{\text{sec}}^{sum} = t - \frac{t^2}{2Ne^{-t}} - \Delta + \frac{\Delta^2}{2Ne^{-t}}. \quad (16)$$

Taking a derivative from R_{sec}^{sum} in (16) with respect to (w.r.t.) t, and equating the result to zero, gives,

$$2Ne^{-t} = 2t + t^2 - \Delta^2, \quad (17)$$

which can be further simplified to,

$$t = \log(2N) - 2\log\log N + \frac{\Delta^2}{(\log N)^2} + O_N(\frac{\log\log N}{\log N}). \quad (18)$$

Now, remembering the term $\nu\sqrt{Ne^{-t}}$ in the equation (14) and incorporating the initial approximation used for deriving (16), R_{sec}^{sum} can be written as follows,

$$R_{\text{sec}}^{sum} = t - \Delta - \frac{t^2 - \Delta^2}{2(\text{N}e^{-t} - \nu\sqrt{Ne^{-t}})}. \quad (19)$$

Again, taking a derivative from R_{sec}^{sum} in (19) w.r.t. t and equating it to zero, leads to,

$$2(Ne^{-t} - \nu\sqrt{Ne^{-t}})^2 - 2t(Ne^{-t} - \nu\sqrt{Ne^{-t}}) - (t^2 - \Delta^2)(Ne^{-t} \quad \frac{\nu}{2}\sqrt{Ne^{-t}}) = 0 \quad (20)$$

After some mathematics, one can write the parameter t as follows,

$$t = \log 2N + \log(1 - \frac{\nu}{\sqrt{Ne^{-t}}}) - \log(t^2 - \Delta^2) + \log(1 - \frac{\nu}{\sqrt{Ne^{-t}}} - \frac{t}{Ne^{-t}}) - \log(1 - \frac{\nu}{2\sqrt{Ne^{-t}}}). \quad (21)$$

Plugging the result of (18) as an initial point into the right-hand side of (21), and after some mathematics we can arrive at,

$$t = \log\ (2N) - 2\log\log N + \frac{\Delta^2}{(\log N)^2} + 4(\frac{\log\log N}{\log N}) + O_N(\frac{\nu}{\log N}). \quad (22)$$

The result of (22) can be further simplified to (23), by the assumption of $\nu = O(\log\log N)$ as follows,

$$t = \log(2N) - 2\log\log N + \frac{\Delta^2}{(\log N)^2} + O_N(\frac{\log\log N}{\log N}). \quad (23)$$

which can be considered as the optimal link activation threshold value. Substituting the result of (22) into (19), the asymptotic achievable secrecy rate can be formulated as follows,

$$R_{\text{sec}}^{sum} = \log\frac{2N}{M} - 2\log\log N + O_N(\frac{\Delta^2}{(\log N)^2} + \frac{\log\log N}{\log N}). \quad (24)$$

The result of (24) declares that, in order to have a non-vanishing secrecy rate the following relation should be satisfied,

$$\log\frac{2N}{M} - 2\log\log N >> 0 \quad (25)$$

The inequality (25) implies that the order of the eavesdroppers is restricted to,

$$M = o_N(\frac{N}{(\log N)^2}). \quad (26)$$

It is worth mentioning that considering the maximum order of the eavesdroppers in (26) and the result of (23) for the link activation threshold, the validity of the assumption of having a large number of active links in each transmission block, in the beginning of this section can be verified. Moreover, considering (26), the maximum channel strength associated with the eavesdroppers can be formulated as follows,

$$\Delta = o_N(\log\frac{N}{(\log N)^2} + o_N(\log\frac{N}{(\log N)^2})) = o_N(\log\frac{N}{(\log N)^2}). \quad (27)$$

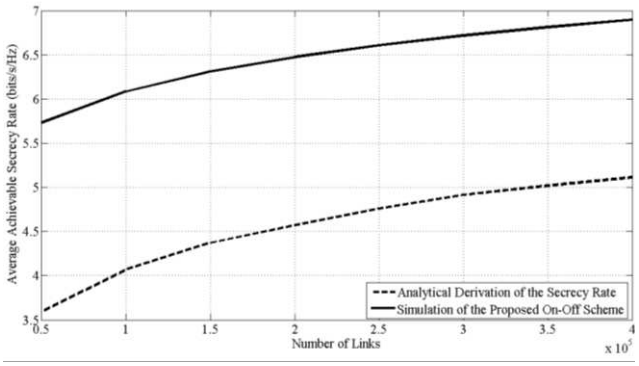

Figure 2. Acheivable sum secrecy rate, associated with the proposed ON/OFF method.

Comparing the derived relation for Δ to the last terms of t and R_{sec}^{sum} in (23) and (24), one can neglect re-write the optimal link activation value and the achievable sum secrecy rate as follows,

$$t = \log(2N) - 2\log\log N + O_N(\frac{\log\log N}{\log N}). \quad (28)$$

$$R_{\text{sec}}^{sum} = \log\frac{2N}{M} - 2\log\log N + O_N(\frac{\log N.\log\log N}{(\log N)^2}). \quad (29)$$

IV. Simulation Results

In this section, we aim at demonstrating that the average achievable secrecy rate of the considered network has the same behavior as the asymptotic secrecy rate derived in (24). In this regard, a network consisting of N transmitter-receiver pairs in the presence of $M = 40$ eavesdroppers is considered. The number of transmitter-receiver pairs is swept from 5×10^4 to $4 \times 10\text{^}5$. The channel coefficients between any transmitter and receiver is drawn from a circularly symmetric Gaussian random variable of unit variance and the additive noise of $\mathcal{CN}(0,1)$ is assumed to be present at each receiver. The simulation result of Fig.2 demonstrates that the asymptotic sum secrecy rate of the network has the same behavior as average achievable secrecy rate, derived from simulation.

V. Conclusion

The achievable secrecy rate of a decentralized network is considered throughout this paper. It is shown that in a Rayleigh flat fading environment, where N legitimate transmitter-receiver pairs are communicating to each other in the presence of M eavesdroppers. In this regard, an on-off transmission protocol is proposed that aims at maximizing the achievable secrecy rate in the network. Accordingly, the achievable secrecy rate as well as the limitation on the number of eavesdroppers to have non-vanishing sum secrecy rate are addressed.

References

[1] P.Gupta and P. R. Kumar, "The capacity of wireless," *IEEE Transactions on Information Theory,* vol. 46, no. 2, pp, 388-404, March 2000.

[2] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 4, pp. 477 – 486, Aug.2002.

[3] S. Toumpis and A. J. Goldsmith, "Large wireless networks under fading, mobility, and delay constraints," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, 2004, p. 619.

[4] S. Cui, A. M. Haimovich, O. Somekh, H. V. Poor and S. Shamai, "Throughput scaling of wireless networks with random connections," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3793 –3806, Aug.2010.

[5] O.O. Koyluoglu, C.E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE TRANSACTIONS ON INFORMATION THEORY*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[6] M. Mirmohseni and P. Papadimitratos, "Scaling laws for secrecy capacity in cooperative wireless networks," in *IEEE INFOCOM 2014- IEEE Conference on Computer Communications*, 2014.

[7] J. Zhang, L. Fu and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *IEEE/ACM Transactions on Networking*, vol. 22, no. 1, pp. 66–79, Feb. 2014.

[8] M. Mirmohseni A. H. Hadavi, N. Kazempour and M. R. Aref, "Secrecy capacity in large cooperative networks in presence of eavesdroppers with unknown locations," in *Iran Workshop on Communication and Information Theory (IWCIT)*, 2016.

[9] M. Ebrahimi, M. A. Maddah-Ali and A. K. Khandani, "Throughput scaling laws for wireless networks with fading channels," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4250 – 4254, Nov. 2007.

[10] M. Grossglauser and D. N. C. Tse, "Throughput scaling in decentralized single-hop wireless networks with fading channels," *Technical Report UW-ECE No.2006-13, University of Waterloo*, Aug. 2006.

[11] M. Ebrahimi and A. K. Khandani, "Rate-constrained wireless networks with fading channels: Interference-limited and noise-limited regimes," *IEEE Transactions on Information Theory*, vol. 57, no. 12, pp. 7714 – 7732, Dec. 2011.

[12] S. P. Shariatpanahi, B. H. Khalaj, K. Alishahi and H. Shah-Mansouri, "Throughput of large one-hop ad hoc wireless networks with general fading," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 7, pp. 3304 – 3310, July. 2015.

[13] T. M. Cover and J. A. Thomas, *Elements of information theory*, Wiley Interscince, 2006.