On Secrecy Rates and Outage in Multi-User Multi-Eavesdroppers MISO Systems

Joseph Kampeas, Asaf Cohen and Omer Gurewitz
Ben-Gurion University of the Negev, Beer-Sheva, 84105, Israel
Email: {kampeas,coasaf,gurewitz}@bgu.ac.il

Abstract—In this paper, we study the secrecy rate and outage probability in Multiple-Input-Single-Output (MISO) Gaussian wiretap channels at the limit of a large number of legitimate users and eavesdroppers. In particular, we analyze the asymptotic achievable secrecy rates and outage, when *only statistical knowledge* on the wiretap channels is available to the transmitter.

The analysis provides exact expressions for the reduction in the secrecy rate as the *number of eavesdroppers grows*, compared to the boost in the secrecy rate as *the number of legitimate users grows*.

I. INTRODUCTION

The explosive expansion of wireless communication and wireless based services is leading to a growing necessity to provide privacy in such systems. Due to the broadcast nature of the transmission, wireless networks are inherently susceptible to eavesdropping. One of the most promising techniques to overcome this drawback is utilizing Physical-Layer security. Physical-layer security leverages the random nature of communication channels to enable encoding techniques such that eavesdroppers with inferior channel quality are unable to extract any information about the transmitted information from their received signal [1]–[3].

Many recent studies have explored the potential gains in exploiting multiple antenna technology for attaining secrecy in various setups. For example, in the case of a single eavesdropper, when the transmitter has a full Channel State Information (CSI) on the wiretap channel, it can ensure inferior wiretap channel by nulling the reception on the eavesdropper's end, thus, achieve higher secrecy rates [4]–[6]. When the user and eavesdropper are also equipped with multiple antennas, the optimal strategy is to utilize linear precoding in order to focus energy only in few directions, thus achieving the optimal secrecy rate [7]. In case that *only statistical information* on the wiretap channel is available, the optimal scheme is beamforming in the user's direction [4], [8]. However, in this case, a *secrecy outage*, the event that at the eavesdropper is able to extract all or part of the message,

is unavoidable. To mitigate risk, one should consider transmitting Artificial Noise (AN) to further degrade the wiretap channel [9]–[13].

The secrecy capacity *at the limit of large number of antennas* was considered in [9], [10]. Particularly, [9], [10] studied the asymptotic (in the number of cooperating antennas) secrecy capacity, for a single receiver. [14] used Extreme Value Theory (EVT) to study the scaling law of the secrecy sum-rate under a random beamforming scheme, when the users and eavesdroppers *are paired*. That is, each user was susceptible to eavesdropping only by its paired (single) eavesdropper. [15] considered the asymptotic secrecy rate, where both the number of users and number of antennas grow to infinity, while all users are potentially malicious and few external eavesdroppers are wiretapping to the transmissions.

In the presence of a single user and multiple eavesdroppers, where the transmitter has no CSI on the wiretap channels, a secrecy outage will definitely occur as the number of eavesdroppers goes to infinite [16]. On the other hand, when there are many legitimate users, and the transmitter can select users opportunistically, the secrecy outage probability is open in general. In particular, the asymptotically exact expression to the number of users required in order to attain sufficiently small secrecy outage probability, is yet to be solved.

This study analyzes this subtle relation between the number of users, eavesdroppers and the resulting secrecy outage probability. Specifically, we consider the secrecy rate and outage probability for the Gaussian MISO wiretap channel model, where a transmitter is serving K legitimate users in the presence of M eavesdroppers, and analyze the secrecy outage probability as a function of K and M, and more importantly, the relation between these two numbers.

We assume that CSI is available from all legitimate users, yet *only channel statistics* are available on the eavesdroppers. As previously mentioned, when the transmitter has only statistical information on the wiretap channel, transmitting in the direction of the attending

user is optimal when AN is not allowed. Moreover, in large scale systems, using AN may interfere with other cells, and probably would not be a method of choice even at the price of reduced secrecy rate. Beamforming to the attending user, on the other hand, is the de-facto transmission scheme in many MISO systems today. Therefore, we adopt the scheme in which at each transmission opportunity the transmitter beamforms in the direction of a user with favorable channel. We analyze the asymptotics of the secrecy rate and secrecy outage under the aforementioned scheme. In particular, our contributions are as follows: (i) We first analyze the secrecy rate distribution when transmitting to the strongest user while many eavesdroppers are wiretapping. These results are utilized to attain the secrecy outage probability in the absence of the wiretap channels' CSI. (ii) We provide both upper and lower bounds on the limiting secrecy rate distribution. The bounds are tractable and give insight on the scaling law and the effect of the system parameters on the secrecy capacity. We show via simulations that our bounds are tight. (iii) We quantify the reduction in the secrecy rate as the *number of eavesdroppers grows*, compared to the boost in the secrecy rate as *the number of legitimate users grows*. We show that in order to attain asymptotically small secrecy outage probability with t transmit antennas, $\Omega\left(n\left(\log n\right)^{t-1}\right)$ users are required in order to compensate for n eavesdroppers in the system.

II. SYSTEM MODEL

Throughout this paper, we use bold lower case letters to denote random variables and random vectors, unless stated otherwise. $V^\dagger$ denotes the Hermitian transpose of matrix V. Further, $|\cdot|$, $\langle\cdot,\cdot\rangle$ and $\|\cdot\|$ denote the absolute value of a scalar, the inner product and the Euclidean norm of vectors, respectively.

Consider a MISO downlink channel with one transmitter with t transmit antennas, K legitimate users with a single antenna and M uncooperative eavesdroppers, again, with one antenna each. The transmitter adopts the scheme in which at each transmission opportunity the transmitter beamforms in the direction of the selected user without AN. We assume a block fading channel where the transmitter can query for fine channel reports from the users before each transmission, while having *only statistical knowledge on the wiretap channels*.

Let $\mathbf{y}_i$ and $\mathbf{z}_j$ denote the received signals at user i and at eavesdropper j, respectively. Then, the received signals can be described as $\mathbf{y}_i = \mathbf{h}_i\mathbf{x} + \mathbf{n}_{b(i)}$ and $\mathbf{z}_j = \mathbf{g}_j\mathbf{x} + \mathbf{n}_{e(j)}$, where $\mathbf{h}_i \in \mathbb{C}^{t\times 1}$ and $\mathbf{g}_j \in \mathbb{C}^{t\times 1}$ are the channel vectors between the transmitter and user i, and between the transmitter and eavesdropper j, respectively.

$\mathbf{h}_i$ and $\mathbf{g}_j$ are random complex Gaussian channel vectors, where the entries have zero mean and unit variance in the real and imaginary parts. $\mathbf{x} \in \mathbb{C}^t$ is the transmitted vector, with a power constraint $\mathrm{E}\left[\mathbf{x}^\dagger\mathbf{x}\right] \leq P$, while $\mathbf{n}_{b(i)}, \mathbf{n}_{e(j)} \in \mathbb{C}$ are unit variance Gaussian noises seen at user i and eavesdropper j, respectively.

The secrecy capacity for the Gaussian MIMO wiretap channel, where the main and wiretap channels, $\mathbf{H}$ and $\mathbf{G}$, respectively, are known at the transmitter, was given in [7], [10]

$$C_s = \max_{\Sigma_\mathbf{x}} \log\det\left(I + \mathbf{H}\Sigma_\mathbf{x}\mathbf{H}^\dagger\right) - \log\det\left(I + \mathbf{G}\Sigma_\mathbf{x}\mathbf{G}^\dagger\right) \tag{1}$$

with $\mathrm{tr}\left(\Sigma_\mathbf{x}\right) \leq P$. For the special case of Gaussian MISO wiretap channel, (1) reduces to

$$C_s = \max_{\Sigma_\mathbf{x}} \log\det\left(I + \mathbf{h}\Sigma_\mathbf{x}\mathbf{h}^\dagger\right) - \log\det\left(I + \mathbf{g}\Sigma_\mathbf{x}\mathbf{g}^\dagger\right).$$

In both Gaussian MIMO and MISO, the optimal $\Sigma_\mathbf{x}$ is *low rank*, which means that to achieve the secrecy capacity, the optimal strategy is *transmitting in few directions*. Specifically, for the Gaussian MISO wiretap channel, the capacity achieving strategy is beamforming to a single direction, hence, letting $\mathbf{w}$ denote a beam vector, then $\Sigma_\mathbf{x} = \mathbf{w}\mathbf{w}^\dagger$, [4]. Moreover, when the wiretap channel is unknown at the transmitter, it is optimal to beamform in the direction of the main channel, i.e., $\mathbf{w} = \hat{\mathbf{h}} = \mathbf{h}/\|\mathbf{h}\|$, [4], [8].

Accordingly, when beamforming in the direction of the user while the eavesdropper is wiretapping, assuming only the main channel is known to transmitter, the secrecy capacity is [16], [17]:

$$\mathbf{R}_s(\mathbf{h}, \mathbf{g}) = \log\left(\frac{1 + P\|\mathbf{h}\|^2}{1 + P|\langle\hat{\mathbf{h}}, \mathbf{g}\rangle|^2}\right). \tag{2}$$

Recall that in the block fading environment, $\mathbf{h}$ and $\mathbf{g}$ are random variables and are drawn from the Gaussian distribution independently after each block (slot). Hence, the distribution of the ratio in (2) and its support are critical to obtain important performance metrics. In particular, the *ergodic secrecy rate*, i.e., the secrecy rate when considering coding over a large number of time-slots, can be obtained by computing an expectation with respect to the fading of both $\mathbf{g}$ and $\mathbf{h}$. Similarly, a certain target secrecy rate R_s is achievable if the instantaneous ratio in (2) is greater than the matching value. On the other hand, a *secrecy outage* occurs if R_s is greater than the instantly achievable secrecy rate $\mathbf{R}_s(\mathbf{h}, \mathbf{g})$, and thus, the message cannot be delivered securely [17]. The probability of such event is $\mathrm{Pr}\left(\mathbf{R}_s(\mathbf{h}, \mathbf{g}) < R_s\right)$.

For clarity, let us point out a few statistical properties of the ratio in (2). In the denominator, the squared inner

product $|\langle \hat{\mathbf{h}}, \mathbf{g} \rangle|^2$ follows the Chi-squared distribution with 2 degrees of freedom, $\chi^2(2)$ (which is equivalent to the Exponential distribution with rate parameter 1/2), since $\hat{\mathbf{h}}$ is normalized, rotating both $\hat{\mathbf{h}}$ and $\mathbf{g}$ such that $\hat{\mathbf{h}}$ aligns with the unit vector does not change the inner product. Thus, the inner product result in a complex Gaussian random variable [18], [19]. Similarly, in the numerator, the squared norm $\|\mathbf{h}\|^2$ follows the Chi-squared distribution with $2t$ degrees of freedom, $\chi^2(2t)$, since it is a sum of t squared complex Gaussian random variables. Thus, for any user i and eavesdropper j, the secrecy SNR when beamforming to user i is equivalent to the ratio of $1+\chi^2(2t)$ and $1+\chi^2(2)$ random variables.

A. Main Tool

To assess the ratio in the presence of large number of users and eavesdroppers, let us recall that for sufficiently large n, the maximum of a sequence of n i.i.d. $\chi^2(v)$ variables, $\mathbf{M}_n = \max(\boldsymbol{\xi}_1, ..., \boldsymbol{\xi}_n)$ follows the Gumbel distribution [20, pp. 156]. Specifically, $\lim_{n\to\infty} \Pr(\mathbf{M}_n \le a_n \xi + b_n) = \exp\{-e^{-\xi}\}$, where a_n and b_n are normalizing constants. In this case,

$$a_n = 2, \tag{3}$$

$$b_n = 2\left(\log n + \left(\frac{v}{2} - 1\right)\log\log n - \log\Gamma\left[\frac{v}{2}\right]\right) \tag{4}$$

and $\Gamma[\cdot]$ is the Gamma function.

In this paper, we study the asymptotic (in the number of users and eavesdroppers) distribution of the ratio in (2), and thus derive the secrecy outage probability, *when the transmitter schedules a user with favorable CSI and beamforms in its direction.*

III. ASYMPTOTIC SECRECY OUTAGE

In this section, we analyze the secrecy outage limiting distribution. That is, for a given target secrecy rate R_s, we analyze the probability that *at least one eavesdropper among M eavesdroppers* will attain information from the transmission. Obviously, when transmitting to a *single user*, and when only statistical knowledge is available on the wiretap channels, beamforming to the user whose channel gain is the greatest among K users is optimal.

Accordingly, let $i^* = \arg\max_i \|\mathbf{h}_i\|^2$ be the index of the channel with the largest gain, and let $j^* = \arg\max_j |\langle \hat{\mathbf{h}}_{i^*}, \mathbf{g}_j \rangle|^2$ be the index of the wiretap channel whose projection in the direction $\hat{\mathbf{h}}_{i^*}$ is the largest. Note that when the transmitter beamforms to user i^* in a multiple eavesdroppers environment, it should tailor a code with secrecy rate R_s to protect the message even from the strongest eavesdropper with respect to i^*, which

is j^*. Of course, with only statistical information on the eavesdroppers, j^* is unknown to the transmitter. Accordingly, the probability of a secrecy outage when transmitting to user i^* at secrecy rate R_s is [17]:

$$\Pr\left(\log_2\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle \hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*} \rangle|^2}\right) \le R_s\right)$$

$$= \Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle \hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*} \rangle|^2} \le 2^{R_s}\right) \tag{5}$$

To ease notation, we denote $\alpha = 2^{R_s}$.

In the following, we analyze the distribution in (5) when the number of users and eavesdroppers is large. In particular, we consider the secrecy rate distribution when the transmitter beamforms to user i^*, while all eavesdroppers are striving to intercept the transmission separately (without cooperation).

When the transmitter is beamforming to a user whose channel gain is the greatest, then the squared norm $\|\mathbf{h}_{i^*}\|^2$ in the numerator of (5) scales with the number of users like $O(\log K)$ [20]. Nevertheless, the greatest channel projection in the direction of the attending user, in the denominator of (5), also scales with the number of eavesdroppers in the order of $O(\log M)$. Moreover, asymptotically, both the greatest gain and greatest channel projection follow the Gumbel distribution (with different normalizing constants). Thus, in order to determine the secrecy rate behavior, as K and M grow, one needs to address the ratio of Gumbel random variables. However, the ratio distribution of Gumbel random variables is not known to have a closed-form [21]. Thus, we first express it as an infinite sum of Gamma functions, then provide tight bounds on the obtained distribution, from which we can infer the outage probability. Accordingly, we have the following.

Theorem 1. *For large enough K and M, the distribution of the secrecy rate in (5) is the following.*

$$\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle \hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*} \rangle|^2} \le \alpha\right)$$

$$= \sum_{k=0}^{\infty} \frac{(-1)^k e^{-(k+1)\frac{1+b_K - \alpha(1+b_M)}{\alpha a_M}}}{(k+1)!} \Gamma\left[1 + \frac{(k+1)a_K}{\alpha a_M}\right]$$

where a_K, a_M and b_K, b_M are normalizing constants given in (3) and (4), respectively.

Note that b_K and b_M grow at different rate. Specifically, although b_K and b_M are both normalizing constant of the χ^2 distribution, b_K has value of $v = 2t$ in (4)), while b_M has value of $v = 2$ in (4). The proof is given in the Appendix.

3

To evaluate the result in Theorem 1, one needs to evaluate the infinite sum, which is intricate. Thus, the following upper and lower bounds are useful.

A. Bounds on the Secrecy Rate Distribution

In the following, we suggest an approach that models EVT according to its tail distribution, which enables us to provide tight bounds to the distribution in (5). This approach has very clear and intuitive *communication interpretation*. Specifically, for an upper bound, we put a threshold on eavesdropper j^*'s wiretap channel projection, and analyze the result under the assumption that its projection exceeded. For a lower bound, we put a threshold on user i^*'s channel gain, and analyze the result under the assumption that its gain has exceeded it.

When only a single user (eavesdropper), among many, exceeds a threshold on average, then the above-threshold tail distribution corresponds to the tail of extreme value distribution [22, Ch. 4.2]. Moreover, the tail limiting distribution has a mean value that is higher than the mean value of the extreme value distribution, since the tail limiting distribution takes into account only events in which user i^* (eavesdropper j^*) is sufficiently strong, namely, above threshold. Thus, replacing the extreme value distribution of user i^* (eavesdropper j^*) with its corresponding tail distribution will increase the numerator (denominator) in (5) on average. Thus, the resulting secrecy rate is higher (lower), hence, corresponds to a lower (upper) bound on the ratio CDF.

Let u_m denote a threshold on the wiretap channel projection in the direction $\hat{\mathbf{h}}_{i^*}$, such that a single (the strongest) eavesdropper exceeds it on average. Note that such a threshold can be obtained by inversing the complement CDF of the Exponential distribution. Further, note that this inverse is exactly (4) with $v = 2$ degrees of freedom. Accordingly, we have the following lower bound.

Lemma 1. *For sufficiently large K and M, the CDF of the secrecy rate in (5) satisfies the following upper bound.*

$$
\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle\hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2} \le \alpha\right)
$$
$$
\le \frac{a_K}{\alpha a_M} e^{-\frac{1 + b_K - \alpha(1 + u_m)}{\alpha a_M}} \Gamma\left[\frac{a_K}{\alpha a_M}, 0, e^{\frac{1 + b_K - \alpha(1 + u_m)}{a_K}}\right],
$$

where $\Gamma[s, 0, z] = \int_0^z \tau^s e^{-\tau} d\tau$ is the lower incomplete Gamma function.

The proof is given in the Appendix. The following corollary helps gaining insights from Lemma 1.

Corollary 1. *For $\alpha \ge 1$, the outage probability satisfies the following bound.*

$$
\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle\hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2} \le \alpha\right)
$$
$$
< \left[\Lambda(\alpha)\left(1 - \exp\left\{-\Lambda(\alpha)^{-1} 2^{\alpha-1}\right\}\right)\right]^{1/\alpha},
$$

where $\Lambda(\alpha) = (\sqrt{e}M)^\alpha \frac{\Gamma(t)}{\sqrt{e}K(\log K)^{t-1}}$.

Note that the value of $\Lambda(\alpha)$ determines the outage probability. In particular, at the limit $\Lambda(\alpha) \to \infty$, the resulting outage probability is 1 (i.e., when $M \to \infty$ and K is fixed). Similarly, when $\Lambda(\alpha) \to 0$, the resulting outage probability 0. Moreover, we point out that $\Lambda(\alpha)$ is decreasing with the number of users as $K(\log K)^{t-1}$, while increasing with the number of eavesdroppers as M^α. Thus, roughly speaking, as long as the number of eavesdroppers $M = o\left(K(\log K)^{t-1}\right)^{1/\alpha}$, we obtain $\Lambda(\alpha) = o(1)$, hence, secrecy outage in the order of $o(1)$.

To prove Corollary 1, the following Claim is useful.

Claim 1 ([23]–[25]). *The incomplete Gamma function satisfies the following bounds.*

(i) $\Gamma[s](1 - e^{-z})^s \quad < \quad \Gamma[s, 0, z] \quad <$ $\Gamma[s]\left(1 - e^{-z\Gamma[1+s]^{-1/s}}\right)^s, \forall \quad 0 < s < 1.$ *This inequality takes the opposite direction for values of $s > 1$.*

(ii) $2^{s-1} \le \Gamma[1+s] \le 1, \forall \quad 0 < s < 1.$

(iii) $\Gamma[s]\Gamma[1/s] \ge 1, \forall s > 0.$

    Proof: (Corollary 1). Applying the normalizing constants in (3)-(4) to Lemma 1 result in

$$
\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle\hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2} \le \alpha\right)
$$
$$
\le \frac{1}{\alpha}\left(\frac{(\sqrt{e}M)^\alpha \Gamma[t]}{\sqrt{e}K(\log K)^{t-1}}\right)^{\frac{1}{\alpha}} \Gamma\left[\frac{1}{\alpha}, 0, \frac{\sqrt{e}K(\log K)^{t-1}}{(\sqrt{e}M)^\alpha \Gamma[t]}\right]
$$

To ease notation, let us denote $\Lambda(\alpha) = \frac{(\sqrt{e}M)^\alpha \Gamma(t)}{\sqrt{e}K(\log K)^{t-1}}$. Thus, we rewrite Lemma 1 as

$$
\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle\hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2} \le \alpha\right)
$$
$$
\le \frac{1}{\alpha}\Lambda(\alpha)^{1/\alpha}\Gamma\left[\frac{1}{\alpha}, 0, \Lambda(\alpha)^{-1}\right]
$$
$$
\overset{(a)}{<} \frac{1}{\alpha}\Lambda(\alpha)^{1/\alpha}\Gamma\left[\frac{1}{\alpha}\right]\left(1 - e^{-\frac{\Gamma\left[1+\frac{1}{\alpha}\right]^{-\alpha}}{\Lambda(\alpha)}}\right)^{1/\alpha}
$$
$$
\overset{(b)}{\le} \left[\Lambda(\alpha)\left(1 - e^{-\frac{2^{\alpha-1}}{\Lambda(\alpha)}}\right)\right]^{1/\alpha}
$$

Remember that only $\alpha \geq 1$ implies secrecy rate greater than zero. Thus, (a) follows from Claim $1(i)$, and (b) follows from Claim $1(ii)$ and from the Gamma function recurrence property, $\Gamma\left[\frac{1}{\alpha}\right] = \alpha\Gamma\left[1 + \frac{1}{\alpha}\right]$. ∎

For the lower bound, we utilize a similar approach, however, this time, we refer to user i^* as if its channel gain has exceeded a high threshold. Thus, since only sufficiently strong user i^*, whose gain is above threshold, is taken into account, then the numerator in (5) is larger on average, thus, resulting in a higher rate, which corresponds to a lower bound on the ratio CDF.

Let u_k denote a threshold on the user's channel gain, such that a single strongest user exceeds it on average. Note that such a threshold can be obtained from the inverse incomplete Gamma function, which asymptotically, is exactly (4) with $v = 2t$. Accordingly, we have the following upper bound.

Lemma 2. *For sufficiently large K and M, the CDF of the secrecy rate in (5) satisfies the following lower bound.*

$$\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle \hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2} \leq \alpha\right) \geq 1 - \frac{\alpha a_M}{a_K}$$

$$\cdot e^{-\frac{\alpha(1+b_M)-(1+u_k)}{a_K}} \Gamma\left[\frac{\alpha a_M}{a_K}, 0, e^{-\frac{1+u_k-\alpha(1+b_M)}{\alpha a_M}}\right].$$

The proof is given in the Appendix.
Again, to gain intuition, we have the following.

Corollary 2. *For $\alpha \geq 1$, the outage probability satisfies the following bound.*

$$\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle \hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2} \leq \alpha\right)$$
$$> 1 - \Gamma\left[1 + \alpha\right]\Lambda(\alpha)^{-1}\left(1 - e^{-\Lambda(\alpha)^{1/\alpha}}\right)^\alpha,$$

where $\Lambda(\alpha) = \left(\sqrt{e}M\right)^\alpha \frac{\Gamma(t)}{\sqrt{e}K(\log K)^{t-1}}$.

Proof: Similar to Corollary 1, we apply the normalizing constants in (3)-(4) to Lemma 2, then, set $\Lambda(\alpha) = \frac{\left(\sqrt{e}M\right)^\alpha\Gamma(t)}{\sqrt{e}K(\log K)^{t-1}}$. Thus, we have

$$\Pr\left(\frac{1 + P\|\mathbf{h}_{i^*}\|^2}{1 + P|\langle \hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2} \leq \alpha\right)$$
$$\geq 1 - \alpha\Lambda(\alpha)^{-1}\Gamma\left[\alpha, 0, \Lambda(\alpha)^{1/\alpha}\right]$$
$$\overset{(a)}{>} 1 - \alpha\Lambda(\alpha)^{-1}\Gamma\left[\alpha\right]\left(1 - e^{-\Lambda(\alpha)^{1/\alpha}}\right)^\alpha$$
$$\overset{(b)}{=} 1 - \Gamma\left[1 + \alpha\right]\Lambda(\alpha)^{-1}\left(1 - e^{-\Lambda(\alpha)^{1/\alpha}}\right)^\alpha$$
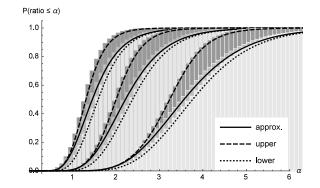

Fig. 1. Simulation and analysis of the ratio distribution in (5) for $M = K = 30$ and $t = 2, 4, 8$ antennas, left to right, respectively. The solid line represents the sum of the first 100 terms in Theorem 1. The dashed and dotted lines represent the distribution upper and lower bounds given in Lemma 1 and Lemma 2, respectively.

where (a) follows form Claim $1(i)$ and (b) follows from the Gamma function recurrence property. ∎

IV. SIMULATION RESULTS

In this section, we present simulate results for the suggested scheduling scheme and compare them to the analysis.

Figure 1 depicts the distribution of the ratio in (5) for three cases and compare it to the analytical results herein. In particular, we simulate the secrecy rate in (2) for three cases: (i) When beamforming to strongest user i^*, while the strongest, above-threshold, eavesdropper is wiretapping, (ii) when beamforming to strongest user i^*, while strongest eavesdropper j^* is wiretapping (without threshold constraint). (iii) when beamforming to strongest, above-threshold, user, while the strongest eavesdropper j^* is wiretapping. The dark gray, gray and light gray bars represents these results, respectively. Then we evaluate the bounds given in Lemma 1 and Lemma 2 and compare then to the sum of the first 100 terms in Theorem 1, for $t = 2, 4, 8$ and $M = K = 30$. It is clear the bounds are tight and provide excellent approximation to (5). For comparison between the bounds given in Corollary 1, Lemma 1, Lemma 2 and Corollary 2, for $t = 4$, $M = K = 1000$, see Figure 2.

Figure 3 depicts the secrecy outage probability. In particular, we set $t = 4$ and $\alpha = 2$, and fix the number of users to $K = 1000$. Then we examine what is the secrecy outage probability as a function of the number of eavesdroppers. The dots represents the critical ratio between M and K such that $\Lambda(\alpha) = 1$, which is exactly $M = \Theta\left(K\left(\log K\right)^{t-1}\right)^{1/\alpha}$. Indeed, for values of M which have smaller order than the critical value, result
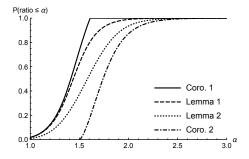
5

Fig. 2. A comparison between the bounds given in Corollary 1, Lemma 1, Lemma 2 and Corollary 2, respectively, for $t = 4$, $M = K = 1000$.
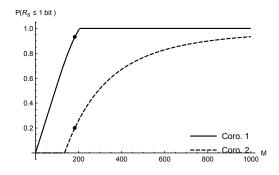

Fig. 3. The upper and lower bounds given in Corollary 1 and Corollary 2, for $K = 1000$, $t = 4$ and $\alpha = 2$, as a function of the number of eavesdroppers M. The marked dot represents the critical ratio where $\Lambda(\alpha) = 1$.

in small values of $\Lambda(\alpha)$, hence, small outage probability.

V. CONCLUSION

We have studied the secrecy rate and outage probability in the presence of multiple legitimate users and eavesdroppers for the complex Gaussian MISO channel, in which only statistical knowledge on the wiretap channels is available to the transmitter. Specifically, we analyzed the secrecy rate distribution when transmitting to the strongest user while many eavesdroppers are wiretapping, and derived the resulting secrecy outage probability. We showed that the secrecy rate in such transmission scheme behaves like the ratio of Gumbel distributions, which does not have a closed form expression. Thus, tight upper and lower bounds on the limiting secrecy rate distribution were given. These bounds are tractable and provide insight on the scaling law and the effect of the system parameters on the secrecy capacity. In particular, the reduction in the secrecy rate as the *number of eavesdroppers grows*, compared to the boost in the secrecy rate as *the number of legitimate users grows* was quantified, and we proved that in the presence of n eavesdroppers,

to attain asymptotically small secrecy outage probability with t transmit antennas, $\Omega\left(n(\log n)^{t-1}\right)$ legitimate users are required. To support our claims, we conducted rigorous simulations that shows that our bounds are tight.

APPENDIX

A. Proof of Theorem 1

First, note that in (5), the squared norm in the numerator and the squared inner product in the denominator are independent. Specifically, while the former represents the length of the user's channel, the latter represents the square of the product of the eavesdropper channel's magnitude and the cosine of the phase between the eavesdropper's channel and the user's channel. Since the angle between i.i.d. Gaussian vectors is independent of their norms [26], the distribution of the squared inner product in the denominator is identical for all eavesdroppers and independent of the user index.

Accordingly, to ease notation, let $\boldsymbol{\gamma}_{i^*} = P\|\mathbf{h}_{i^*}\|^2$ and let $\boldsymbol{\gamma}_{j^*} = P|\langle\hat{\mathbf{h}}_{i^*}, \mathbf{g}_{j^*}\rangle|^2$. Note that, asymptotically, as both are maximum of series of random variables, they have extreme type distributions, e.g., $\boldsymbol{\gamma}_{i^*} \sim \mathrm{G}(Pa_K, Pb_K)$ and $\boldsymbol{\gamma}_{j^*} \sim \mathrm{G}(Pa_M, Pb_M)$, where $\mathrm{G}(a_n, b_n)$ denotes the Gumbel distribution with the normalizing constants a_n and b_n, given in (3) and (4), respectively. Further, let us define the ratio transform $\boldsymbol{\alpha} = \frac{1+\boldsymbol{\gamma}_{i^*}}{1+\boldsymbol{\gamma}_{j^*}}$ and $\boldsymbol{\beta} = \boldsymbol{\gamma}_{j^*}$, with the inverse transform, $\boldsymbol{\gamma}_{i^*} = \boldsymbol{\alpha}(1+\boldsymbol{\beta}) - 1$. Accordingly, we have,

$$\Pr\left(\boldsymbol{\alpha} > \alpha, \boldsymbol{\beta} > \beta\right) = \Pr\left(\boldsymbol{\gamma}_{i^*} > \alpha(1+\boldsymbol{\gamma}_{j^*}) - 1, \boldsymbol{\gamma}_{j^*} > \beta\right)$$

$$= \int_\beta^\infty f_{\boldsymbol{\gamma}_{j^*}}(\gamma_j)\left(1 - F_{\boldsymbol{\gamma}_{i^*}}\left(\alpha(1+\gamma_j) - 1\right)\right)\mathrm{d}\gamma_j$$

$$= \left(1 - F_{\boldsymbol{\gamma}_{j^*}}(\beta)\right) - \int_\beta^\infty f_{\boldsymbol{\gamma}_{j^*}}(\gamma_j)F_{\boldsymbol{\gamma}_{i^*}}\left(\alpha(1+\gamma_j) - 1\right)\mathrm{d}\gamma_j$$

Noting that $f_{\boldsymbol{\gamma}_{j^*}}(\gamma) = \frac{1}{a_M}e^{-\frac{\gamma - b_M}{a_M}}e^{-e^{-\frac{\gamma - b_M}{a_M}}}$ and $F_{\boldsymbol{\gamma}_{i^*}}(\gamma) = e^{-e^{-\frac{\gamma - b_K}{a_K}}}$, we exchange variables such that $e^{-\frac{\gamma - b_M}{a_M}} = \zeta$, hence, $\gamma = -a_M\log(\zeta) + b_M$ and $\mathrm{d}\gamma = \frac{-a_M}{\zeta}\mathrm{d}\zeta$. Further, we note that $\left(\zeta \cdot e^{-\frac{b_M}{a_M}}\right)^{\frac{\alpha a_M}{a_K}}$ is equal to $e^{-\frac{\alpha\gamma}{a_K}}$, which is useful for this case. Accordingly, we have,

$$\Pr\left(\boldsymbol{\alpha} > \alpha, \boldsymbol{\beta} > \beta\right) = \left(1 - F_{\boldsymbol{\gamma}_{j^*}}(\beta)\right)$$

$$- \int_0^{e^{-\frac{\beta - b_M}{a_M}}} e^{-\zeta}\exp\left\{-e^{\frac{1+b_K - \alpha(1+b_M)}{a_K}} \cdot \zeta^{\frac{\alpha a_M}{a_K}}\right\}\mathrm{d}\zeta$$

Generally, this integral cannot be reduced to a closed-form. However, if we replace $e^{-\zeta}$ with its series expansion and noting that we can interchange the sum and the

integral from Fubini's theorem, we have,

$$\Pr\left(\boldsymbol{\alpha} > \alpha, \boldsymbol{\beta} > \beta\right) = \left(1 - F_{\boldsymbol{\gamma}_{j*}}(\beta)\right) - \sum_{k=0}^{\infty} \frac{1}{k!}$$

$$\cdot \int_0^{e^{-\frac{\beta - b_M}{a_M}}} (-\zeta)^k e^{-e^{\frac{1+b_K - \alpha(1+b_M)}{a_K}} \cdot \zeta^{\frac{\alpha a_M}{a_K}}} \mathrm{d}\zeta$$

$$= \left(1 - F_{\boldsymbol{\gamma}_{j*}}(\beta)\right)$$

$$- \frac{a_K}{\alpha a_M} \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \left(e^{\frac{1+b_K - \alpha(1+b_M)}{a_K}}\right)^{-\frac{(k+1)a_K}{\alpha a_M}}$$

$$\cdot \Gamma\left[\frac{(k+1)a_K}{\alpha a_M}, 0, e^{-\frac{\alpha(\beta - b_M)}{a_K}} e^{\frac{1+b_K - \alpha(1+b_M)}{a_K}}\right]$$

where $\Gamma[s, 0, z] = \int_0^z \tau^s e^{-\tau} \mathrm{d}\tau$ is the lower incomplete Gamma function. Finally, since we are only interested in the marginal distribution $\boldsymbol{\alpha}$, we set $\beta \to -\infty$ to obtain,

$$\Pr(\boldsymbol{\alpha} \le \alpha)$$

$$= \frac{a_K}{\alpha a_M} \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} e^{-(k+1)\frac{1+b_K - \alpha(1+b_M)}{\alpha a_M}} \cdot \Gamma\left[\frac{(k+1)a_K}{\alpha a_M}\right]$$

$$\tag{6}$$

$$= \sum_{k=0}^{\infty} \frac{(-1)^k}{(k+1)!} e^{-(k+1)\frac{1+b_K - \alpha(1+b_M)}{\alpha a_M}} \cdot \Gamma\left[1 + \frac{(k+1)a_K}{\alpha a_M}\right]$$

$$\tag{7}$$

where the last step follows from the identity $x\Gamma[x] = \Gamma[x+1]$ for all $x > 0$. Thus, Theorem 1 follows.

B. Proof of Lemma 1

Denote $\mathcal{E} = \left\{j : |\langle \hat{\mathbf{h}}_{i*}, \mathbf{g}_j \rangle|^2 > u_m\right\}$. Notice that $0 \le |\mathcal{E}| \le M$.

When an eavesdropper sees above-threshold channel projection, then the excess above the threshold follows the exponential distribution with rate $1/a_M$ [22, Ch. 4.2]. To ease notation, let $\boldsymbol{\gamma}_{i*} = \|\mathbf{h}_{i*}\|^2$ and let $\boldsymbol{\gamma}_{\bar{j}} \in \mathcal{E}$. Accordingly, $\boldsymbol{\gamma}_{i*} \sim G(a_K, b_K)$ and $\boldsymbol{\gamma}_{\bar{j}} \sim Exp\left[1/a_M\right]$. Let us define variables transformation $\boldsymbol{\alpha} = \frac{1 + \boldsymbol{\gamma}_{i*}}{1 + u_m + \boldsymbol{\gamma}_{\bar{j}}}$ and $\boldsymbol{\beta} = \boldsymbol{\gamma}_{\bar{j}}$, for which the inverse is $\boldsymbol{\gamma}_{i*} = \boldsymbol{\alpha}(1 + u_m + \boldsymbol{\gamma}_{\bar{j}}) - 1$. Accordingly, we have

$$\Pr\left(\boldsymbol{\alpha} > \alpha, \boldsymbol{\beta} > \beta\right)$$

$$= \Pr\left(\boldsymbol{\gamma}_{\bar{j}} > \beta, \boldsymbol{\gamma}_{i*} > \alpha\left(1 + u_m + \boldsymbol{\gamma}_{\bar{j}}\right) - 1\right)$$

$$= \int_\beta^\infty f_{\boldsymbol{\gamma}_{\bar{j}}}(\gamma_j)\left(1 - F_{\boldsymbol{\gamma}_{i*}}\left(\alpha\left(1 + u_m + \boldsymbol{\gamma}_{\bar{j}}\right) - 1\right)\right) \mathrm{d}\gamma_j$$

$$= \left(1 - F_{\boldsymbol{\gamma}_{\bar{j}}}(\beta)\right)$$

$$- \int_\beta^\infty f_{\boldsymbol{\gamma}_{\bar{j}}}(\gamma_j) F_{\boldsymbol{\gamma}_{i*}}\left(\alpha\left(1 + u_m + \gamma_j\right) - 1\right) \mathrm{d}\gamma_j$$

Noting that $f_{\boldsymbol{\gamma}_{\bar{j}}}(\gamma) = e^{-\gamma/a_M}/a_M$ and $F_{\boldsymbol{\gamma}_{i*}}(\gamma) = e^{-e^{-\frac{\gamma - b_K}{a_K}}}$, we exchange variables such that $e^{-e^{-\frac{\alpha\gamma_j}{a_K}}} = \zeta$,

hence, $\gamma_j = -\frac{a_K}{\alpha}\log(\zeta)$ and $\mathrm{d}\gamma_j = -\frac{a_K}{\alpha\zeta}\mathrm{d}\zeta$. Further, note that $e^{-\frac{\gamma_j}{a_M}}$ is equal to $\zeta^{\frac{a_K}{\alpha a_M}}$. Thus, we have,

$$\Pr\left(\boldsymbol{\alpha} > \alpha, \boldsymbol{\beta} > \beta\right) = \left(1 - F_{\boldsymbol{\gamma}_{\bar{j}}}(\beta)\right)$$

$$- \int_0^{e^{-\frac{\alpha\beta}{a_K}}} \frac{a_K}{\alpha a_M} \zeta^{\frac{a_K}{\alpha a_M} - 1} \cdot e^{-e^{\frac{1+b_K - \alpha(1+u_m)}{a_K}}} \cdot \zeta \mathrm{d}\zeta$$

$$= \left(1 - F_{\boldsymbol{\gamma}_{\bar{j}}}(\beta)\right) - \frac{a_K}{\alpha a_M}$$

$$\cdot e^{-\frac{1+b_K - \alpha(1+u_m)}{\alpha a_M}} \Gamma\left[\frac{a_K}{\alpha a_M}, 0, e^{\frac{1+b_K - \alpha(1+u_m + \beta)}{a_K}}\right]$$

To obtain the marginal distribution of the ratio $\boldsymbol{\alpha}$, we set $\beta = 0$, to obtain

$$\Pr\left(\boldsymbol{\alpha} > \alpha\right)$$

$$= 1 - \frac{a_K}{\alpha a_M} e^{-\frac{1+b_K - \alpha(1+u_m)}{\alpha a_M}} \Gamma\left[\frac{a_K}{\alpha a_M}, 0, e^{\frac{1+b_K - \alpha(1+u_m)}{a_K}}\right]$$

Note that a u_m can be calculated from the inverse exponential distribution. Namely, $u_m = 2\log(M)$. Note also that for such a threshold the probability that exactly one (strongest) eavesdropper is above-threshold is

$$\Pr\left(|\mathcal{E}| = 1\right) = (1 - 1/M)^{M-1} \to e^{-1} \approx 0.37.$$

Further,

$$\Pr\left(|\mathcal{E}| > 1\right) = 1 - \left((1 - 1/M)^{M-1} + (1 - 1/M)^M\right)$$

$$\to 1 - 2e^{-1} \approx 0.26.$$

Thus, given that some eavesdroppers are above threshold, it is most likely that only one has exceeded.

C. Proof of Lemma 2

Denote $\mathcal{U} = \left\{i : \|\mathbf{h}_i\|^2 > u_k\right\}$.

When a user sees above-threshold squared channel norm, then the excess above the threshold, in this case as well, follows the exponential distribution with rate $1/a_K$ [22, Ch. 4.2]. To ease notation, let $\boldsymbol{\gamma}_{\bar{i}} \in \mathcal{U}$ and let $\boldsymbol{\gamma}_{j*} = |\langle \hat{\mathbf{h}}_{i*}, \mathbf{g}_{j*} \rangle|^2$. Accordingly, $\boldsymbol{\gamma}_{j*} \sim G(a_M, b_M)$ and $\boldsymbol{\gamma}_{\bar{i}} \sim Exp\left[1/a_K\right]$. Let us define variables transformation $\boldsymbol{\alpha} = \frac{1 + u_k + \boldsymbol{\gamma}_{\bar{i}}}{1 + \boldsymbol{\gamma}_{j*}}$ and $\boldsymbol{\beta} = \boldsymbol{\gamma}_{j*}$, for which the inverse is $\boldsymbol{\gamma}_{\bar{i}} = \boldsymbol{\alpha}(1 + \boldsymbol{\gamma}_{j*}) - (1 + u_k)$. Accordingly, we have

$$\Pr\left(\boldsymbol{\alpha} > \alpha, \boldsymbol{\beta} > \beta\right)$$

$$= \Pr\left(\boldsymbol{\gamma}_{\bar{i}} > 0, (1 + u_k + \boldsymbol{\gamma}_{\bar{i}})/\alpha - 1 > \boldsymbol{\gamma}_{j*} > \beta\right)$$

$$= \int_0^\infty f_{\boldsymbol{\gamma}_{\bar{i}}}(\gamma_i)\left(F_{\boldsymbol{\gamma}_{j*}}\left(\frac{1 + u_k + \boldsymbol{\gamma}_{\bar{i}}}{\alpha} - 1\right) - F_{\boldsymbol{\gamma}_{j*}}(\beta)\right) \mathrm{d}\gamma_i$$

$$= \int_0^\infty f_{\boldsymbol{\gamma}_{\bar{i}}}(\gamma_i) F_{\boldsymbol{\gamma}_{j*}}\left(\frac{1 + u_k + \boldsymbol{\gamma}_{\bar{i}}}{\alpha} - 1\right) \mathrm{d}\gamma_i - F_{\boldsymbol{\gamma}_{j*}}(\beta)$$

Noting that $f_{\boldsymbol{\gamma}_{\bar{i}}}(\gamma) = e^{-\gamma/a_K}/a_K$ and $F_{\boldsymbol{\gamma}_{j*}}(\gamma) = e^{-e^{-\frac{\gamma - b_M}{a_M}}}$, we exchange variables such that $e^{-e^{-\frac{\gamma_i}{\alpha a_M}}} =$

ζ, hence, $\gamma_i = -\alpha a_M \log(\zeta)$ and $\mathrm{d}\gamma_i = -\frac{\alpha a_M}{\zeta} \mathrm{d}\zeta$. Further, note that $e^{-\frac{\gamma_i}{a_K}}$ is equal to $\zeta^{\frac{\alpha a_M}{a_K}}$. Thus, we have,

$$\Pr\left(\boldsymbol{\alpha} > \alpha, \boldsymbol{\beta} > \beta\right)$$

$$= \int_0^1 \frac{\alpha a_M}{a_K} \zeta^{\frac{a_K}{\alpha a_M}-1} \cdot e^{-\zeta e^{-\frac{1+u_k-\alpha(1+b_M)}{\alpha a_M}}} \mathrm{d}\zeta - F_{\boldsymbol{\gamma}_{j*}}(\beta)$$

$$= \frac{\alpha a_M}{a_K} e^{\frac{1+u_k-\alpha(1+b_M)}{a_K}} \Gamma\left[\frac{\alpha a_M}{a_K}, 0, e^{-\frac{1+u_k-\alpha(1+b_M)}{\alpha a_M}}\right]$$
$$\quad - F_{\boldsymbol{\gamma}_{j*}}(\beta)$$

Setting $\beta \to -\infty$, the marginal distribution of $\boldsymbol{\alpha}$ follows.

Note that a u_k can be calculated from the inverse regularized Gamma function. Note that u_k can also be approximated from b_K. Herein, it is also most likely that exactly one (strongest) user exceeded for such threshold.

REFERENCES

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

[2] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, 1978.

[3] S. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, 1978.

[4] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*. IEEE, 2007, pp. 2466–2470.

[5] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel," *Information Theory, IEEE Transactions on*, vol. 55, no. 9, pp. 4033–4039, 2009.

[6] G. Geraci, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO linear precoding," in *Wireless Communication Systems (ISWCS), 2011 8th International Symposium on*. IEEE, 2011, pp. 286–290.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Information Theory, IEEE Transactions on*, vol. 57, no. 8, pp. 4961–4972, 2011.

[8] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 4, pp. 1176–1187, 2011.

[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 7, pp. 3088–3104, 2010.

[10] ——, "Secure transmission with multiple antennas-part II: The MIMOME wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5515–5532, 2010.

[11] S. A. Fakoorian, A. L. Swindlehurst *et al.*, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1701–1713, 2013.

[12] J. H. Lee and W. Choi, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure dof and jammer scaling law," *Signal Processing, IEEE Transactions on*, vol. 62, no. 4, pp. 828–839, Feb 2014.

[13] C. Wang, H. Wang, X. Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *Wireless Communications, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[14] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *Signal Processing Letters, IEEE*, vol. 20, no. 2, pp. 141–144, 2013.

[15] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 5, pp. 2931–2943, 2014.

[16] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*. IEEE, 2007, pp. 1301–1305.

[17] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *Information Theory, 2006 IEEE International Symposium on*. IEEE, 2006, pp. 356–360.

[18] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *Information Theory, IEEE Transactions on*, vol. 51, no. 2, pp. 506–522, 2005.

[19] K. P. Jagannathan, S. Borst, P. Whiting, and E. Modiano, "Efficient scheduling of multi-user multi-antenna systems," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2006 4th International Symposium on*. IEEE, 2006, pp. 1–8.

[20] P. Embrechts, C. Klüppelberg, and T. Mikosch, *Modelling extremal events: for insurance and finance*. Springer, 2011, vol. 33.

[21] S. Nadarajah and A. H. El-Shaarawi, "On the ratios for extreme value distributions with application to rainfall modeling," *Environmetrics*, vol. 17, no. 2, pp. 147–156, 2006.

[22] S. Coles, *An introduction to statistical modeling of extreme values*. Springer Verlag, 2001.

[23] W. Gautschi, "The incomplete gamma functions since tricomi," in *In Tricomi's Ideas and Contemporary Applied Mathematics, Atti dei Convegni Lincei, n. 147, Accademia Nazionale dei Lincei*. Citeseer, 1998.

[24] A. Laforgia and P. Natalini, "On some inequalities for the gamma function," *Advances in Dynamical Systems and Applications*, vol. 8, no. 2, pp. 261–267, 2013.

[25] C. Mortici, "New sharp bounds for gamma and digamma functions," *An. Stiint. Univ. AI Cuza Iasi Ser. N. Mat*, vol. 56, no. 2, 2010.

[26] J. Kampeas, A. Cohen, and O. Gurewitz, "MAC capacity under distributed scheduling of multiple users and linear decorrelation," in *Proceedings of the Information Theory Workshop (ITW), Seville, Spain*. IEEE, 2013, pp. 1–5.