Physical layer security in wireless networks with passive and active eavesdroppers

Arsenia Chorti, Samir M. Perlaza, Zhu Han, H. Vincent Poor

Physical Layer Security in Wireless Networks with Passive and Active Eavesdroppers

Arsenia Chorti[†,*], Samir M. Perlaza[†], Zhu Han[‡], H. Vincent Poor[†]
[†]Dep. EE, Equad 19 Olden Street, Princeton University, Princeton, New Jersey 08544, USA
[*]ICS-FORTH N. Plastira 100, Vassilika Vouton, GR-700 13 Heraklion, Crete, Greece
[‡]Dep. ECE, N324, Engineering Building 1, University of Houston, Houston, TX 77004.
{achorti, perlaza, poor}@princeton.edu, zhan2@mail.uh.edu

***Abstract*—Security is becoming an increasingly important issue in wireless communications, to which physical layer approaches can contribute by providing addition resources for securing confidential messages. In this paper, the resilience of multi-user networks to passive and active eavesdropping is investigated. In particular, average secrecy capacities are evaluated in scenarios involving a base station and several terminals, some of which constitute *passive* or *active* eavesdroppers. Network resources (e.g. power) are allocated by the base station based on the available channel state information. The average secrecy capacity of such a network is evaluated in the following cases: (i) in the presence of passive eavesdroppers when no side information is available to the base station; (ii) in the presence of passive eavesdroppers with side information available; and (iii) in the presence of a single active eavesdropper with side information available. This investigation demonstrates that substantial secrecy rates are attainable in the presence of passive eavesdroppers as long as minimal side information, e.g. a statistical characterization of the *number* of potential eavesdroppers, is available to the base station. On the other hand, it is further found that active eavesdroppers can potentially compromise such networks unless statistical inference is employed to restrict their ability to attack.**

I. Introduction

Physical layer security has re-emerged as a focal point of research in information and communication theory due to the importance of its potential applications. Building on the pioneering works of Wyner [1] and Csiszár and Körner [2], it has been demonstrated that a noisy communication channel offers opportunities for perfectly secret communication [3] as long as a legitimate user has a signal-to-noise ratio (SNR) advantage with respect to an eavesdropper. In particular, it has been shown that in situations where the eavesdropper's channel is on average a degraded version of the main channel, a positive secrecy capacity (SC) can be guaranteed. Extending these results, analyses for the wireless fading channel [4], [5] [6] and multiple-input multiple-output (MIMO) systems [7] establish positive secrecy capacities even when on average the eavesdropper's channel can be better than that of the legitimate user.

Nevertheless, physical layer security is still considered a primarily theoretical area of research as only few practical systems proposals have yet come to light. In this paper, we explore network planning options towards this direction. We investigate multi-user networks in which a base station (BS) manages the available resources, e.g. allocates the channel to a user and decides on the transmission power level. We explore the network resilience to passive and active eavesdropping when side information might or might not be available to the BS. Our findings indicate that a substantial average SC is attainable when as little information as an expectation on the *number* of passive eavesdroppers is available. On the other hand, it is shown that the effect of active eavesdroppers can be detrimental and network performance can potentially be severely degraded. In order to deal with such malicious behavior, the BS needs to have access to a larger amount of side information concerning the statistical characterization of the *behavior* of active eavesdroppers. Intuitively, a fiercer type of attack requires stronger defence mechanisms.

The paper is organized as follows: our system model is outlined in Section II. The scenario of passive eavesdropping without available side information is examined in Section III, while in Section IV we present results when side information regarding the number of passive eavesdroppers is available. In Section V, we investigate the case of active eavesdropping, which we formulate as a one-shot two player zero-sum game. Finally, Section VI concludes the paper.

II. System Model

We consider the downlink of a single cell network with a set $\mathcal{K} = \{1, \ldots, K\}$ of $K = |\mathcal{K}|$ receiving terminals. Furthermore, by $h_{k,i}$ we denote the slow fading channel realization between the BS and the k-th terminal during the i-th communication frame (time indices are henceforth omitted). We assume that for all $k \in \mathcal{K}$, h_k are instances of a zero-mean circularly symmetric complex Gaussian random process with unit variance. As a result, the channel gain between the BS and receiver k is $g_k = |h_k|^2$ and follows an exponential distribution $f(g_k)$ with $\mathbb{E}[|h_k|^2] = 1$, i.e.,

$$f(g_k) = e^{-g_k}, k \in \mathcal{K}. \quad (1)$$

Finally, the cumulative distribution function (cdf) of the random variable g_k is denoted by $F(g_k)$, where

$$F(g_k) = 1 - e^{-g_k}, k \in \mathcal{K}. \quad (2)$$

Based on the channel state information (CSI) reported by subscribed users, the BS estimates their SNRs γ_k and selects

This work was supported in part by the IOF "APLOE" (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community and in part by the Qatar National Research Fund (QNRF) and U.S. National Science Foundation Grants CCF-1016671, CNS-0905556, CNS-1117560, CNS-0953377 and ECCS-1028782.

to transmit a codeword x_k - drawn from a Gaussian codebook - with power $p = \mathbb{E}[x_k^2] \in \{0, p_{\max}\}$ to the subscribed user with the highest SNR. This user will in the following be denoted with index a, so that

$$a = \arg\max_{k \in \mathcal{K}} \gamma_k. \quad (3)$$

The objective of the BS is to transmit secret messages even in the presence of passive or active eavesdroppers. Amongst the set $\mathcal{E} = \{1, \ldots, E\}$ of E eavesdroppers, we denote with index $e \in \mathcal{E}$ the one with the highest SNR during a given channel realization, i.e.,

$$e = \arg\max_{k \in \mathcal{E}} \gamma_k. \quad (4)$$

During this transmission, the signals received by the intended and any other terminal are, respectively, expressed as

$$y_a = h_a x_a + w_a, \quad (5)$$
$$y_k = h_k x_a + w_k, k \in \mathcal{E} \cup \mathcal{K} \backslash \{a\}, \quad (6)$$

where the terms w_i are zero-mean unit-variance circularly symmetric complex Gaussian noise. Thus, the individual SNRs are expressed as

$$\gamma_k = g_k p, k \in \mathcal{E} \cup \mathcal{K}. \quad (7)$$

Based on the above, it is straightforward to show that during a particular communication frame the SC is expressed as

$$C_s = \left(\log \frac{1 + \gamma_a}{1 + \gamma_e} \right)^+, \quad (8)$$

where $(\cdot)^+ = \max(\cdot, 0)$. In the following sections, we treat a number of scenarios separately. First, we consider the case in which the transmitter has no side information regarding the existence or identity of potential eavesdroppers. Second, we consider the case in which an estimate of the number of passive eavesdroppers is provided. Finally, the scenario of a single active eavesdropper is investigated.

III. Average SC without Side Information

In this section, we examine the case where the BS has no side information regarding the existence of eavesdroppers; in this scenario, the set of users $\mathcal{K}$ can be extended to include *any* terminal that can act as an eavesdropper (invoking that potentially $K \to \infty$). In this setting, the average SC strictly depends on the SNR difference of the terminal with the highest SNR in respect to the terminal with the second highest SNR. For ease of notation, we denote the latter with the index b, i.e.,

$$b = \arg\max_{k \in \mathcal{K} \backslash \{a\}} \gamma_k. \quad (9)$$

Furthermore, to simplify the analysis we assume that the channel realizations are independent and identically distributed (i.i.d.). Thus, the probability density functions (pdf) $f_a(g_a)$ and $f_b(g_b)$ of the channel gains g_a and g_b, respectively, are the K-th and $(K-1)$-th order statistics of a sample of K channel realizations [8], [9], [10],

$$f_a(g_a) = K F(g_a)^{K-1} f(g_a), \quad (10)$$
$$f_b(g_b) = K(K-1) F(g_b)^{K-2} (1 - F(g_b)) f(g_b), \quad (11)$$

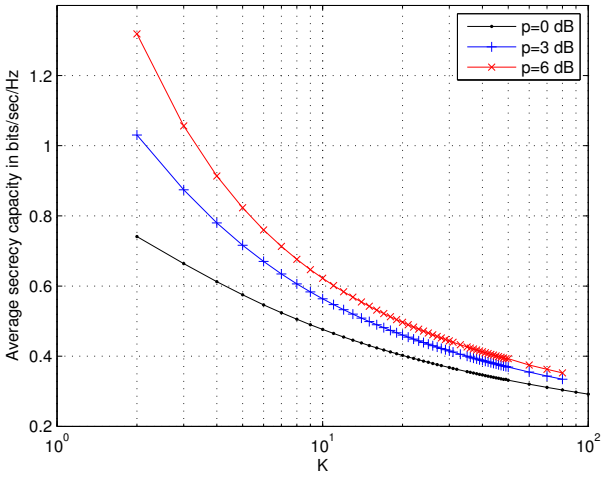

Fig. 1. Average secrecy capacity when the BS has no side information as a function of K.

with cdfs $F_a(g_a)$ and $F_b(g_b)$, respectively. g_a and g_b are generated through a *common* ordering operation which is clearly a nonlinear transformation. As a result, they are not independent [11]. Based on the general expression for the joint pdf of any two order statistics, the joint pdf of g_a and g_b is derived as

$$f_{ab}(g_a, g_b) = K(K-1) F(g_b)^{K-2} f(g_b) f(g_a). \quad (12)$$

Generalizing the reasoning presented in [4] and [5], we find that the average SC without side information at the BS is expressed as follows:

Proposition 1 (Average SC without side information): The average SC of a network of K terminals in a wide-sense stationary channel is given by

$$\langle C_s \rangle = \int_0^{+\infty} \int_0^{g_a} \log \left(\frac{1 + g_a p_{\max}}{1 + g_b p_{\max}} \right) f_{ab}(g_a, g_b) \mathrm{d}g_b \mathrm{d}g_a. \quad (13)$$

Numerical evaluations[1] of the average secrecy capacity are depicted in Fig. 1. It is important to note that the average SC reduces monotonically with the cardinality K of $\mathcal{K}$. This is due to the fact that the probability of finding two terminals with similar SNR levels increases monotonically with K. Thus, from (13) it becomes clear that in the absence of any side information, the broadcasting of secret messages can be compromised, unless a substantial decrease in the transmission rate can be tolerated. In the following section, we investigate the SC of the system when side information is available at the BS.

IV. Average SC with Side Information

In this section, we consider the situation in which there exists a set $\mathcal{E}$ (disjoint with the set $\mathcal{K}$) of eavesdroppers that wish to decode secret messages. Nevertheless, although the individual identities of the eavesdroppers are not known, side information is available regarding the cardinality $E = |\mathcal{E}|$ of

[1] All numerical integrations hereafter were executed in MAPLE 15 ®.

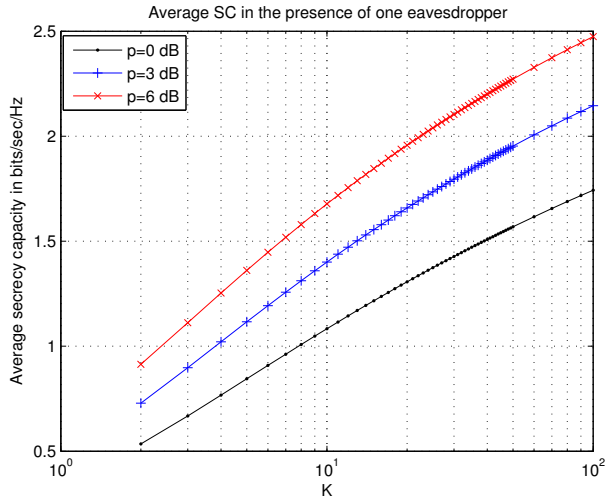

Fig. 2. Average secrecy capacity when the BS has side information over the existence of a single, $E = 1$, eavesdropper as a function of K.

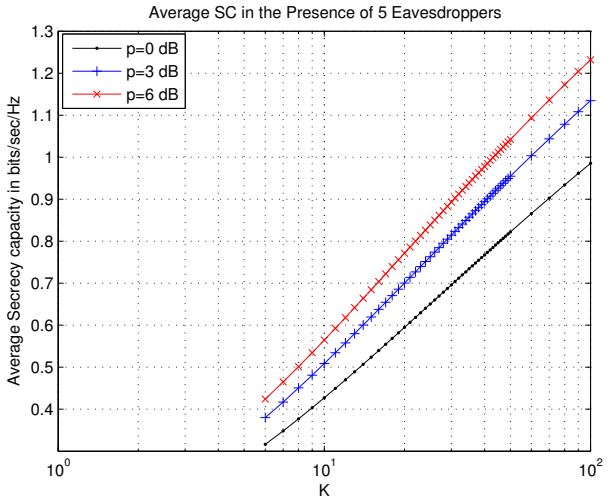

Fig. 3. Average secrecy capacity when the BS has side information over the existence of $E = 5$ eavesdroppers as a function of K.

the set of potential eavesdropping terminals[2]. Amongst this population, we employ the index e to denote the eavesdropping terminal that has the highest statistical advantage for eavesdropping as denoted in (4). In the present work we further assume that the eavesdroppers are not cooperating while the scenario of colluding eavesdroppers is examined in the journal version of the paper.

The pdf $f_e(g_e)$ of the channel gain g_e is the E-th order statistic of a sample of E channel realizations:

$$f_e\left(g_e\right) = EF(g_e)^{E-1} f(g_e) \tag{14}$$

with cdf $F_e(g_e)$. It is important to note that in the case under examination g_a and g_e are generated from two *independent* ordering operations and are consequently independent. The joint pdf $f_{ae}(g_a, g_e)$ of the channel gain of the strongest user and the strongest eavesdropper is merely the product of the marginal distributions, i.e.,

$$f_{ae}(g_a, g_e) = f_a(g_a) f_e(g_e). \tag{15}$$

Consequently, the average SC of the network with respect to a set $\mathcal{E}$ of eavesdroppers is expressed as follows:

Proposition 2 (Average SC with side information): The average SC of a network of K legitimate users with respect to a set of E passive eavesdroppers in a wide-sense stationary channel is given by

$$\langle C_s^* \rangle = \int_0^{+\infty} \int_0^{g_a} \log\left(\frac{1+g_a p_{\max}}{1+g_e p_{\max}}\right) \mathrm{d}F_e(g_e)\mathrm{d}F_a(g_a), \tag{16}$$

where, $f_a(g_a)\mathrm{d}g_a = \mathrm{d}F_a(g_a)$ and $f_e(g_e)\mathrm{d}g_e = \mathrm{d}F_e(g_e)$, respectively.

Numerical evaluations of (16) are depicted in Figs. 2 and 3 in the presence of $E = 1$ and $E = 5$ eavesdropping terminals. Notably, in the case of single eavesdropper, the SC approaches substantial values as the cell size increases. This results from the substantial increase in the probability of finding a legitimate user with a higher SNR than the eavesdropper. This observation recalls the notion of multi-user diversity [12]. Furthermore, albeit that the SC decreases with increasing number of eavesdroppers, substantial secrecy rates are still attainable when the legitimate users outnumber the eavesdroppers, i.e. $E \ll K$.

[2]In a sense we assume that a statistical characterization of the vulnerability of the wireless network has been performed and priors were extracted.

V. Average SC with Side Information in the Presence of an Active Eavesdropper

Next, we consider the scenario in which a single *active* eavesdropper is registered in the network as a subscribed user and exchanges signaling messages with the BS. For simplicity, it is further assumed that the only objective of this malicious user is to decode private messages of *any* legitimate user (this scenario is a subcase of the Byzantine attack). The information accumulated by the eavesdropper depends on the transmission rate and its equivocation rate, with eavesdropping referring to overhearing other users' data.

In this setting, the eavesdropper should intuitively adopt the following strategy: (i) if it has the highest SNR during a given channel realization, i.e. $\gamma_e > \gamma_a$, then it can report a false SNR $\tilde{\gamma}_e < \gamma_a$ to the BS. If the BS does not identify the forgery, it will transmit a private message x_a to a legitimate user a. In this case, the eavesdropper will be able to at least partially decode x_a; (ii) if the eavesdropper does not have the highest SNR, it might not be able to eavesdrop. In this case, it can report a higher false SNR $\tilde{\gamma}_e > \gamma_a$ claiming network resources from the BS. If the BS chooses to transmit to the eavesdropper, although no private information is leaked, the network resources are wasted as none of the legitimate destinations receives any new information.

In such a setting, it would appear that the legitimate users are completely unprotected against active attacks. Nevertheless, at least in principle, deviations in reported CSIs could be bounded around the true value. For example, in the case of a dense network primarily populated by legitimate users,

the BS can employ statistical tests to isolate malicious nodes [13]. Bearing this in mind, we are interested in investigating the network's resilience to active eavesdroppers. That is, eavesdroppers that can mislead the transmitter by introducing false information about their own SNR.

Let us assume the following: (i) the BS can potentially transmit *only* to the user with the highest *reported* SNR and (ii) the eavesdropper *always* reports an SNR $\tilde{\gamma}_e$ that deviates from its true SNR γ_e by a certain additive quantity ϵ, i.e., $\tilde{\gamma}_e = \gamma_e + \epsilon$. Given these assumptions, we define the following function $u : \mathbb{R}^+ \times \mathbb{R} \to \mathbb{R}$, with

$$\begin{aligned} u(p,\epsilon) &= \log\left(\frac{1+g_a p}{1+g_e p}\right)\mathbb{1}_{\{\gamma_a > \gamma_e+\epsilon\}}, \\ &= \log\left(\frac{1+\gamma_a}{1+\gamma_e}\right)\mathbb{1}_{\{\gamma_a > \tilde{\gamma}_e\}}, \end{aligned} \tag{17}$$

where $\mathbb{1}_{\{\cdot\}}$ denotes the indicator function. The BS should aim at the maximization of u, while the eavesdropper at its minimization.

Discussing the problem in more detail, we identify the following cases: (i) When $\gamma_a > \tilde{\gamma}_e$ and $\gamma_a > \gamma_e$, then $u(\gamma_a, \epsilon) > 0$. Thus, the strict positiveness of u is a necessary and sufficient condition for guaranteeing perfect secrecy. (ii) When $u(\gamma_a, \epsilon) = 0$, the BS either does not transmit at all or it transmits to the eavesdropper. In this case, no private messages are leaked. However, the network efficiency is compromised. (iii) When $u(\gamma_a, \epsilon) < 0$, the eavesdropper is able to partially decode the messages of a legitimate user.

In the following, we study the optimal behavior of the BS and the eavesdropper with respect to the function u, by adopting the assumption of full CSI availability at both the transmitter and eavesdropper. This serves only as a first theoretical approximation to determine secrecy rate bounds under the assumption of fully rational base station and eavesdropper.

A. BS Optimal Strategy

Given the action adopted by the eavesdropper, the optimal action of the BS is to choose its transmit power to maximize the function u in (17). That is, the best response of the transmitter, denoted by $\mathrm{BR}_B : \mathbb{R} \to \{0, p_{\max}\}$, is

$$\mathrm{BR}_B(\epsilon) = \arg \max_{p \in \{0, p_{\max}\}} u(p, \epsilon). \tag{18}$$

Thus, we write

$$\mathrm{BR}_B(\epsilon) = \begin{cases} p_{\max}, & \text{if } \gamma_a > \max(\gamma_e, \gamma_e + \epsilon), \\ 0, & \text{otherwise.} \end{cases} \tag{19}$$

B. Eavesdropper Optimal Strategy

The choices of the eavesdropper consist of reporting a forged SNR $\tilde{\gamma}_e = \gamma_e + \epsilon$, greater or lower than its true SNR value γ_e. Indeed, the optimal choice of $\epsilon \in \mathbb{R}$ is the one that minimizes the function u given the choice on the transmit power $p \in \{0, p_{\max}\}$ made by the BS. We define the best response of the eavesdropper by $\mathrm{BR}_e : \{0, p_{\max}\} \to \mathbb{R}$, where,

$$\mathrm{BR}_e(p) = \arg \min_{e \in \mathbb{R}} u(p, \epsilon). \tag{20}$$

Thus, we write

$$\mathrm{BR}_e(p) = \begin{cases} \hat{\epsilon} & \text{if } \gamma_a > \gamma_e, \\ \check{\epsilon} & \text{otherwise,} \end{cases} \tag{21}$$

where the additive errors $\hat{e}$ and $\check{e}$ must satisfy the following conditions to allow the eavesdropper to mislead the transmitter,

$$\hat{\epsilon} \in (|\gamma_a - \gamma_e|, +\infty), \tag{22}$$

$$\check{\epsilon} \in (-\infty, -|\gamma_a - \gamma_e|). \tag{23}$$

We remark that according to the given formulation, for any action adopted by the BS, the eavesdropper has infinite choices in ϵ. Observing (19) and (21), we conclude that the best strategy for the BS as well as the eavesdropper depends on each other's actions. Thus, in the following, we use game theoretic tools to investigate this competitive interaction.

C. Two Player Game Formulation

We model the competitive interaction between the BS and the eavesdropper by the following one-shot two-player zero sum game:

$$\mathcal{G}(g_a, g_e) = \{\mathcal{A}_B, \mathcal{A}_e, u\}. \tag{24}$$

In the course of this game, both g_a and g_e are parameters that are fixed and known to both players. The sets $\mathcal{A}_B$ and $\mathcal{A}_e$ contain the actions available to the BS and the eavesdropper:

$$\mathcal{A}_B = \{0, p_{\max}\}, \tag{25}$$

$$\mathcal{A}_e = \{\hat{\epsilon}, \check{\epsilon}\}. \tag{26}$$

For the sake of simplicity, we assume that both $\hat{\epsilon}$, and $\check{\epsilon}$ are fixed constants such that $\hat{\epsilon} > 0$ and $\check{\epsilon} < 0$. That is, both sets $\mathcal{A}_e$ and $\mathcal{A}_B$ are finite.

The value of u does not depend on the exact value of the additive error ϵ but only on its sign. When the actions p and ϵ are played, the benefit of the transmitter is $u(p, \epsilon)$ while the benefit of the eavesdropper is $-u(p, \epsilon)$. To explore the optimal strategies of the two players, we use the concept of the Nash equilibrium (NE), defined as follows:

Definition 1 (Nash Equilibrium): *The strategy profile $(p^*, \epsilon^*) \in \mathcal{A}_B \times \mathcal{A}_e$ is a Nash equilibrium of the game $\mathcal{G}(g_a, g_e)$ if*

$$p^* \in BR_B(\epsilon^*) \text{ and } \epsilon^* \in BR_e(p^*). \tag{27}$$

Following Def. 1, we state the following lemma.

Lemma 1 (Equilibria in $\mathcal{G}(g_a, g_e)$): *Let $(p^*, \epsilon^*) \in \mathcal{A}_B \times \mathcal{A}_e$ be a Nash equilibrium of the game $\mathcal{G}(g_a, g_e)$, with $\hat{\epsilon} > 0$ and $\check{\epsilon} < 0$. Then,*

- *If $\gamma_a > \gamma_e + \hat{\epsilon}$, then $(p^*, \epsilon^*) \in \{(p_{\max}, \hat{\epsilon}), (p_{\max}, \check{\epsilon})\}$;*
- *If $\gamma_e + \hat{\epsilon} > \gamma_a > \gamma_e$, then $(p^*, \epsilon^*) \in \{(p_{\max}, \hat{\epsilon})\}$;*
- *If $\gamma_e > \gamma_a > \gamma_e + \check{\epsilon}$, then $(p^*, \epsilon^*) \in \{(0, \check{\epsilon})\}$; and*
- *If $\gamma_e + \check{\epsilon} > \gamma_a$, then $(p^*, \epsilon^*) \in \mathcal{A}_B \times \mathcal{A}_e$.*

The proof of Lemma 1 follows immediately from Def. 1. In particular, Lemma 1 indicates that there *always* exists at least one NE for the game $\mathcal{G}(g_a, g_e)$, for all $(g_a, g_e) \in \mathbb{R}^2_+$. Nonetheless, the equilibrium is not necessarily unique. For instance when $\gamma_a > \gamma_e$ and the condition (22) is not met, there exist two NEs: $(p_{\max}, \hat{\epsilon})$ and $(p_{\max}, \check{\epsilon})$. More interestingly, in this case, $u(p_{\max}, \hat{\epsilon}) = u(p_{\max}, \check{\epsilon}) = \log(\frac{1+\gamma_a}{1+\gamma_e}) > 0$. That is,

independently of the forgery of the eavesdropper, it cannot neither obtain a channel allocation so that it avoids the transmitter to send secret information to one of the legitimate receivers nor eavesdrop the communication. Hence, transmitting secret information to the receiver with the highest channel gain, independently of the action of the eavesdropper, is always an NE. In contrast, when $\gamma_a > \gamma_e$ and the condition (22) is met, there exists a unique NE: $(p_{\max}, \hat{\epsilon})$ and $u(p_{\max}, \hat{\epsilon}) = 0$. In this cases, the transmitter decides to transmit but it chooses the eavesdropper as destination as it appears as the receiver with the highest channel gain. Thus, no leak of secret information occurs. However, the eavesdropper introduces a delay for the transmitter to actually communicate with one of the legitimate receivers.

On the contrary, when $\gamma_a < \gamma_e$ and the condition (23) is not met, there exist four NEs. Basically, any possible combination of actions is an NE and more interestingly $u(p_{\max}, \hat{\epsilon}) = 0$ for all $(p_{\max}, \hat{\epsilon}) \in \mathcal{A}_B \times \mathcal{A}_e$. This is due to the fact that the transmitter, if it transmits, always chooses the eavesdropper as destination and thus, no secret information is leaked. However, none of the legitimate receivers is able to receive secret information. On the contrary, when the condition (23) is met, there exists only one NE: $(0, \check{\epsilon})$ and $u(0, \check{\epsilon}) = 0$. Here, the transmitter remains silent and no information is transmitted to any of the destinations.

Thus, when the conditions (22) and (23) are met and even complete information is assumed at both the transmitter and the eavesdropper, the transmitter is unable to convey secret messages to the legitimate destinations at the NE. However, no leak of secret information occurs neither. This implies that when an eavesdropper is able to properly set its additive error term ϵ, it cannot eavesdrop secret messages but it can introduce an infinitely long delay in the network before a legitimate destination receives a secret message.

On the contrary, when the eavesdropper is unable to set up their error terms ϵ following both (22) and (23), then the transmitter is able to convey secret messages to its legitimate receivers as long as $\gamma_a > \gamma_e$. We describe the average secrecy rate (SR) at the NE in the following proposition.

Proposition 3 (Average SR with one active eavesdropper): In the game $\mathcal{G}(g_a, g_e)$ with K legitimate users and a single active eavesdropper, when the conditions (22) *and* (23) *are not satisfied, the average secrecy rate at the NE is*

$$\langle R_s(\hat{\epsilon})\rangle = \int_0^{+\infty} \int_0^{g_a - \frac{\hat{\epsilon}}{p_{\max}}} \log\left(\frac{1+g_a p_{\max}}{1+g_e p_{\max}}\right) \mathrm{d}F(g_e)\mathrm{d}F_a(g_a). \tag{28}$$

Otherwise, when both conditions (22) *and* (23) *are satisfied,*

$$\langle R_s(\hat{\epsilon})\rangle = 0. \tag{29}$$

From Prop. 3, it can be implied that the average SR with respect to the eavesdropper is upper-bounded by $\langle R_s(\hat{\epsilon})\rangle$. Thus, the respective loss in the achievable secrecy rate as a function of the value $\hat{\epsilon}$ is

$$\begin{aligned}\Delta R_s(\hat{\epsilon}) &= \langle C_s^*\rangle - \langle R_s\rangle \\ &= \int_0^{+\infty} \int_{\left(g_a - \frac{\hat{\epsilon}}{p_{\max}}\right)^+}^{g_a} \log\left(\frac{1+g_a p_{\max}}{1+g_e p_{\max}}\right) \mathrm{d}F(g_e)\mathrm{d}F_a(g_a).\end{aligned} \tag{30}$$

The result in (30) shows that the larger $\hat{\epsilon}$ in the interval (22), the more significant the reduction of the secrecy rate is with respect to the case of a passive eavesdropper.

Another interesting point is that

$$\lim_{\hat{\epsilon}\to\infty} \langle R_s(\hat{\epsilon})\rangle = 0, \tag{31}$$

which implies that if the eavesdropper can choose $\hat{\epsilon}$ arbitrarily large, it can fully block the transmission of secret messages in the system. Nonetheless, an unreasonably large difference $|\gamma_a - \gamma_e|$ could be used as an indicator of the existence of malicious behavior and serve as a tool for the identification of active eavesdroppers, e.g. [14], [15].

D. High SNR Characterization

Interestingly, in the high SNR regime, for finite $\hat{\epsilon} < \infty$, the system becomes robust to active attacks, since

$$\lim_{p_{\max}\to\infty} \langle R_s(\hat{\epsilon})\rangle \quad = \lim_{p_{\max}\to\infty} \langle C_s^*\rangle = c > 0, \text{ with}$$

$$c = \int_0^{+\infty} \int_0^{g_a} \log\left(\frac{g_a}{g_e}\right) \mathrm{d}F(g_e)\mathrm{d}F_a(g_a).$$

This implies that in the high SNR regime, the SC of the system is independent of whether the eavesdropper is active or passive. Numerical evaluations of the average SC in the high SNR regime are depicted in Fig. 4. It is clear that in such scenarios opportunities of perfectly secure transmission can be substantiated.

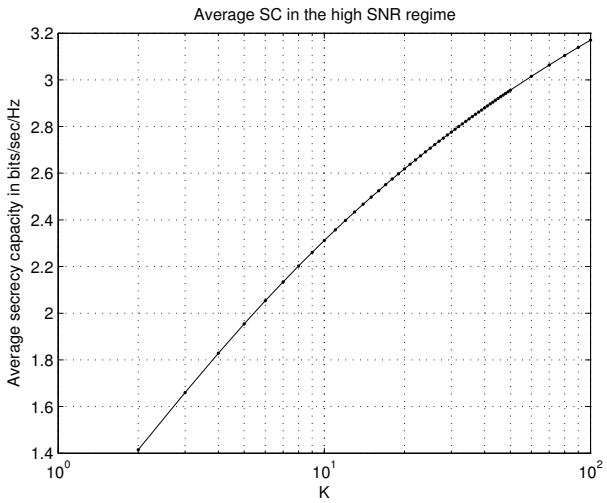

Fig. 4. Average secrecy capacity in the high SNR regime the in the presence of one active or passive eavesdropper as a function of K.

VI. Conclusions

In this paper, we have presented an extensive set of results regarding the characterization of average secrecy capacities in wireless multi-user networks. In our setting, a management unit wishes to transmit secret messages to a set of subscribed users. It has been demonstrated that in absence of any information about the existence of potential eavesdroppers, such an endeavor could be seriously compromised. Nevertheless, if knowledge is available, at least about the number of passive eavesdropping terminals, substantial secrecy rates are attainable. Indeed, achievable secrecy rates increase with the ratio between the number of legitimate users and the number of eavesdroppers. Furthermore, the effect of an active eavesdropper has been systematically evaluated through the use of game theoretic tools. Here, the difference between an active and a passive eavesdroppers is captured by the fact that the former can introduce some false information to mislead the transmitter. For instance, false SNR feedback. Our analysis suggests that in order to minimize the loss incurred by such attacks, extra side information is required. Interestingly, we have found that in the high SNR regime, the network is insensitive to the passiveness or activeness of the attack.

References

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

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

[3] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[5] P. K. Gopala, L. Lifeng, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[6] L. Yingbin, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[7] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[8] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting with multiuser diversity," in *Proc. 44th Annual Allerton Conference on Communication, Control and Computing*, Monticello, IL, Sep. 2006.

[9] J. Hyoungsuk, K. Namshik, C. Jinho, L. Hyuckjae, and H. Jeongseok, "On multiuser secrecy rate in flat fading channel," in *Proc. IEEE Military Communications Conference (MILCOM)*, Boston, MA, Oct. 2009.

[10] M. Z. I. Sarkar and T. Ratnarajah, "Secure communications through rayleigh fading SIMO channel with multiple eavesdroppers," in *Proc. IEEE International Conference on Communications (ICC)*, Cape Town, South Africa, May 2010.

[11] H.-C. Yang and M.-S. Alouini, *Order Statistics in Wireless Communications: Diversity, Adaptation and Scheduling in MIMO and OFDM Systems*. New York, NY: Cambridge University Press, Oct. 2011.

[12] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Proc. IEEE International Conference on Communications (ICC)*, Seattle, WA, Jun. 1995.

[13] A. L. Toledo and W. Xiaodong, "Robust detection of selfish misbehavior in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 6, pp. 1124–1134, Aug. 2007.

[14] A. Algans, K. I. Pedersen, and P. E. Mogensen, "Experimental analysis of the joint statistical properties of azimuth spread, delay spread, and shadow fading," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 3, pp. 523–531, Apr. 2002.

[15] L. Woongsup and C. Dong-Ho, "A new neighbor discovery scheme based on spatial correlation of wireless channel," in *Proc. IEEE Vehicular Technology Conference (VTC-Spring)*, Barcelona, Spain, Apr. 2009.