On the Tradeoffs Between Network State Knowledge and Secrecy

Samir M. Perlaza*, Arsenia Chorti*†, H. Vincent Poor*, and Zhu Han‡

* Dept. of Electrical Engineering, Princeton University, Princeton, NJ, 08544
† Institute of Computer Science, Foundation for Research and Technology - Hellas, Crete, GR 70013, Greece
‡ Dept. of Electrical and Computer Eng., University of Houston, Houston, TX, 77204
Emails: {perlaza, achorti, poor}@princeton.edu, and zhan2@uh.edu

***Abstract*—In this paper, the impact of network-state knowledge on the feasibility of secrecy is studied in the context of non-colluding active eavesdropping. The main contribution is the investigation of several scenarios in which increasing the available knowledge at each of the network components leads to some paradoxical observations in terms of the average secrecy capacity and average information leakage. These observations are in the context of a broadcast channel similar to the time-division downlink of a single-cell cellular system. Here, providing more knowledge to the eavesdroppers makes them more conservative in their attacks, and thus, less harmful in terms of average information leakage. Similarly, providing more knowledge to the transmitter makes it more careful and less willing to transmit, which reduces the expected secrecy capacity. These findings are illustrated with a numerical analysis that shows the impact of most of the network parameters in the feasibility of secrecy.**

I. Introduction

This paper studies the feasibility of secrecy in the context of the downlink of a single-cell cellular system with legitimate and malicious receivers and time-division multiple access. At each time slot, the transmitter decides whether to send information to the receiver with the highest reported signal-to-noise ratio (SNR) or to remain silent. Legitimate receivers report their true SNRs to the transmitters such that the destination selection can take place. Conversely, malicious receivers report a false SNR in order to increase the probability of successful interception of the transmitted data. Reporting a lower SNR than the actual value results in avoiding being selected as the destination, and thus this enables eavesdropping. Reporting a higher value than the actual SNR favors being selected as the destination and therefore, it prevents private information from being sent to legitimate receivers. This problem was introduced in [1] and [2] in the context of active eavesdropping [3]–[7], however the impact of network-state knowledge at each of the network components was not treated. In this paper, the analysis is focused on the importance of the amount of network state knowledge made available to all the network components for them to determine their own strategies. This paper revisits the results presented in [8] and provides numerical examples to highlight the importance of the tradeoffs between network knowledge and the feasibility of secrecy.

This research was supported in part by the Army Research Office under MURI Grant W911NF-11-1-0036, and in part by the Marie Curie International Outgoing Fellowship under Grant FP7-PEOPLE-IOF-2010-274723.

II. Problem Formulation

Consider a transmitter communicating with a set of destinations $\mathcal{D} = \mathcal{K} \cup \mathcal{J}$, following a time-division policy. The destinations in the set $\mathcal{K} = \{1, 2, \ldots, K\}$ are legitimate receivers, while the destinations in the set $\mathcal{J} = \{K+1, \ldots, K+J\}$ are malicious receivers. At every channel use, the transmitter sends information to receiver $i^* \in \mathcal{D}$. When the destination is a legitimate receiver, i.e., $i^* \in \mathcal{K}$, all malicious receivers $j \in \mathcal{J}$ attempt to eavesdrop upon the communication. At every block interval, for all $i \in \mathcal{D}$, the message index $m_i \in \mathcal{M}_i$ is encoded into a codeword $\boldsymbol{x}_i = (x_{i,1}, \ldots, x_{i,N_i}) \in \mathcal{C}_i$, where $\mathcal{M}_i$ and $\mathcal{C}_i$ denote respectively the set of messages and the codebook of the link transmitter-receiver i. For all $\ell \in \{1, \ldots, N_i\}$, $x_{i,\ell}$ are complex and subject to the constraint $\frac{1}{N_i}\mathbb{E}\left[\boldsymbol{x}_i^* \boldsymbol{x}_i\right] \leqslant \bar{P}$, with $\bar{P}$ the average transmit power. The input to receiver i during a given block is denoted by $\boldsymbol{y}_i = (y_{i,1}, \ldots, y_{i,N_i})$ and

$$\boldsymbol{y}_i \quad = \quad h_i \boldsymbol{x}_{i^*} + \boldsymbol{z}_i, \tag{1}$$

where the noise vector is $\boldsymbol{z}_i = (z_{i,1}, \ldots, z_{i,N_i})$; the noise components $z_{i,1}, \ldots, z_{i,N_i}$ and the channel coefficients $h_1, \ldots, h_{K+J}$ are independent circularly symmetric complex Gaussian (CSCG) random variables with zero means and unit variances. The secrecy capacity between the transmitter and a legitimate receiver $k \in \mathcal{K}$ with respect to an eavesdropper $j \in \mathcal{J}$, can be written as follows [9]:

$$C_s(k,j) = \Big(\log(1 + \mathrm{SNR}_k) - \log(1 + \mathrm{SNR}_j) \Big)^+, \tag{2}$$

where $\mathrm{SNR}_i = |h_i|^2 \bar{P}$, for all $i \in \mathcal{D}$. The maximum information leakage rate at eavesdropper j with respect to a legitimate receiver k is denoted by $L_s(k,j)$ and is given by

$$L_s(k,j) = \log(1 + \mathrm{SNR}_j). \tag{3}$$

By assumption $L_s(i,j) = 0$ and $C_s(i,j) = 0$ when $i \in \mathcal{J}$, since the case in which malicious receivers eavesdrop upon malicious receivers is not taken into account as explained in the following.

A. Transmitter's Behavior

At each channel use, the transmitter aims to send information to the receiver for which reliable decoding at the highest achievable secrecy rate is guaranteed. As the transmitter is not able to distinguish a legitimate receiver from a malicious receiver, it simply exploits the multi-user diversity and chooses the receiver i^* with the highest SNR as the destination. The choices of the transmitter are either to transmit with positive power to destination i^* ($\bar{P} = P > 0$), if secrecy can be ensured, or to remain silent ($\bar{P} = 0$), if information leakage might take place. The transmitter obtains the SNRs from all the receivers in advance using regular signaling channels. The vector of reported SNRs is denoted by $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_{K+L})$, where γ_i denotes the SNR reported by receiver i. Then, the index i^* is such that

$$i^* = \arg\max_{i \in \mathcal{D}} \gamma_i. \tag{4}$$

The secrecy capacity at which the transmitter can send information is $C_s(i^*, j^*)$ where j^* is the index of the eavesdropper with the highest potential of eavesdropping [2]:

$$j^* = \arg\max_{j \in \mathcal{J}} \gamma_j. \tag{5}$$

B. Receiver's Behavior

1) Legitimate Receivers: Legitimate receivers always report the actual values of their SNRs, that is $\gamma_k = \mathrm{SNR}_k$, $\forall k \in \mathcal{K}$.

2) Malicious Receivers: All malicious receivers $j \in \mathcal{J}$ aim to eavesdrop upon the communication between the transmitter and a legitimate destination. To achieve this, receiver j does not report its true SNR. It adds an error ϵ such that $\gamma_j = \mathrm{SNR}_j + \epsilon$, and $\epsilon \in \{\hat{\epsilon}, \check{\epsilon}\}$, with $\hat{\epsilon} > 0$ and $\check{\epsilon} < 0$. Note that the exact values of $\hat{\epsilon}$ and $\check{\epsilon}$ are arbitrarily chosen by the eavesdroppers and can be different at each block. More specifically, eavesdropper j might choose the values $\hat{\epsilon}_j$ and $\check{\epsilon}_j$. However, as shown below, only the actions of the eavesdropper j^* influence the behavior of the transmitter. Hence, no indices are used for the values $\hat{\epsilon}$ and $\check{\epsilon}$ in the following. When SNR_{j^*} is the highest SNR in the network, eavesdropper j^* can eavesdrop upon the destination i^*, if this eavesdropper is not chosen as the destination during that time interval. Hence, it reports a lower SNR $\gamma_{j^*} = \mathrm{SNR}_{j^*} + \check{\epsilon}$. In this way, it forces the transmitter to send private information to another receiver more susceptible to eavesdropping. Alternatively, if SNR_{j^*} is not the highest SNR, then its interest is to be selected as the destination such that no private information is sent to other receivers. Note that when a malicious receiver is chosen as the destination after reporting an enhanced SNR, the transmitter might send information at a secrecy rate that cannot be reliably decoded by the destination. Thus, the only objective of the malicious receivers is to eavesdrop upon the legitimate receivers instead of receiving their own information.

C. Network States and Available Knowledge

1) Network States: The global state of the network can be described in terms of the events A and B.

Event A: eavesdropper j^* is able to eavesdrop, i.e., $\mathrm{SNR}_{j^*} > \mathrm{SNR}_{i^*}$; and event B: eavesdropper j^* is able to trick the transmitter, i.e.,

$$\hat{\epsilon} > \left|\mathrm{SNR}_{i^*} - \mathrm{SNR}_{j^*}\right| \text{ and } \check{\epsilon} < -\left|\left(\mathrm{SNR}_{i^*} - \mathrm{SNR}_{j^*}\right)\right|. \tag{6}$$

The feasibility of eavesdropping depends on the events A and B. In state (A, B) eavesdropping is feasible as $\mathrm{SNR}_{j^*} > \mathrm{SNR}_{i^*}$, however, it might not necessarily occur. For instance, if eavesdropper j^* plays $\hat{\epsilon}$, the transmitter chooses the malicious receiver j^* as the destination and no private information crosses the channel. Alternatively, if j^* plays $\check{\epsilon}$ a legitimate receiver might be chosen as the destination and thus, eavesdropping occurs. In state $(A, \bar{B})$, eavesdropper j^* is chosen as the destination. This is basically because, eavesdropper j^* has the highest SNR and it cannot trick the transmitter. In $(\bar{A}, B)$, the eavesdropper j^* can at most mislead the destination selection but cannot eavesdrop since $\mathrm{SNR}_{j^*} < \mathrm{SNR}_{i^*}$. In the state $(\bar{A}, \bar{B})$, a legitimate destination is always selected and strictly positive secrecy rate can be guaranteed as $\mathrm{SNR}_{j^*} < \mathrm{SNR}_{i^*}$ and none of the eavesdroppers can trick the destination selection process.

2) Available Knowledge: A knowledge state (KS) of receiver i (resp. the transmitter) describes the set variables that are known by receiver i (resp. the transmitter). As shown in the next section, the KS of each network element determines its optimal behavior.

a) Transmitter's KS: The transmitter is aware of the presence of active eavesdroppers and possesses estimates of the values of $\hat{\epsilon}$ and $\check{\epsilon}$ using standard tools [10]. However, the transmitter is assumed to be unable to distinguish a legitimate receiver from a malicious receiver and to know whether in the current channel use, it chooses $\epsilon = \hat{\epsilon}$ or $\epsilon = \check{\epsilon}$. Thus, two KSs are considered for the transmitter: $\omega_{\mathrm{Tx}}^{(0)}$ and $\omega_{\mathrm{Tx}}^{(1)}$. At $\omega_{\mathrm{Tx}}^{(0)}$, the transmitter does not know the exact values of K and J, even though it knows the value of $K + J$. Thus, it cannot determine exactly which state, out of all 4 possible states, is the current state of the network. Therefore, from the principle of maximum entropy [11], the beliefs over the network states induced by KS $\omega_{\mathrm{Tx}}^{(0)}$ are uniformly distributed, i.e., $\Pr\left(\cdot, \cdot | \omega_{\mathrm{Tx}}^{(0)}\right) = \frac{1}{4}$.

At $\omega_{\mathrm{Tx}}^{(1)}$, the transmitter knows the exact values of K and J and it knows the distribution of the channel realizations. Thus, the beliefs induced by this KS are

$$\begin{aligned}
\Pr\left(A, B | \omega_{\mathrm{Tx}}^{(1)}\right) &= \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right), \\
\Pr\left(A, \bar{B} | \omega_{\mathrm{Tx}}^{(1)}\right) &= \Pr\left(\mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*} + \check{\epsilon}\right), \\
\Pr\left(\bar{A}, B | \omega_{\mathrm{Tx}}^{(1)}\right) &= \Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*} + \hat{\epsilon}\right), \\
\Pr\left(\bar{A}, \bar{B} | \omega_{\mathrm{Tx}}^{(1)}\right) &= \Pr\left(\mathrm{SNR}_{j^*} + \hat{\epsilon} \leqslant \mathrm{SNR}_{k^*}\right),
\end{aligned}$$

where j^* is defined by (5) and

$$k^* = \arg\max_{k \in \mathcal{K}} \mathrm{SNR}_k. \tag{7}$$

The probability is taken with respect to the distributions of the random variables $|h_{k^*}|^2$ and $|h_{j^*}|^2$ which are the K-th and the J-th order statistics of a set of K and a set of

J samples of independent random variables following a chi-square distribution with 2 degrees of freedom, respectively.

b) Malicious Receivers' KS: A malicious receiver j has two KSs: $\omega_{\mathrm{Rx}}^{(0)}$ and $\omega_{\mathrm{Rx}}^{(1)}$. At $\omega_{\mathrm{Rx}}^{(0)}$, malicious receivers completely ignore the number K of legitimate destinations. Hence, there is no other knowledge available to make a better guess about the network state than a uniform probability distribution [11]. Thus, the beliefs induced by this KS are $\Pr\left(\cdot,\cdot|\omega_{\mathrm{Rx}}^{(0)}\right)=\frac{1}{4}$. At $\omega_{\mathrm{Rx}}^{(1)}$, malicious receivers know the exact number of legitimate receivers K and the distributions of the channels. Therefore, the belief induced by this knowledge state is the following:

$$\Pr\left(A,B|\omega_{\mathrm{Rx}}^{(1)}\right)=\Pr\left(\mathrm{SNR}_{j^*}+\check{\epsilon}<\mathrm{SNR}_{k^*}<\mathrm{SNR}_{j^*}\middle||h_{j^*}|^2\right),$$
$$\Pr\left(A,\bar{B}|\omega_{\mathrm{Rx}}^{(1)}\right)=\Pr\left(\mathrm{SNR}_{k^*}<\mathrm{SNR}_{j^*}+\hat{\epsilon}\middle||h_{j^*}|^2\right),$$
$$\Pr\left(\bar{A},B|\omega_{\mathrm{Rx}}^{(1)}\right)=\Pr\left(\mathrm{SNR}_{j^*}<\mathrm{SNR}_{k^*}<\mathrm{SNR}_{j^*}+\hat{\epsilon}\middle||h_{j^*}|^2\right),$$
$$\Pr\left(\bar{A},\bar{B}|\omega_{\mathrm{Rx}}^{(1)}\right)=\Pr\left(\mathrm{SNR}_{j^*}+\hat{\epsilon}<\mathrm{SNR}_{k^*}\middle||h_{j^*}|^2\right),$$

where j^* and k^* are defined by (5) and (7), respectively. The probability is taken with respect to the distribution of the random variable $|h_{k^*}|^2$. Here, the channel coefficient $|h_j^*|^2$ and thus, the SNR_j^*, are known by receiver j^*.

III. Existing Results

In [8], the interaction between the transmitter and the malicious receivers during a sufficiently large number of independent blocks is modeled by a Bayesian game [12]. In this game, the objectives of the transmitter and the eavesdropper are respectively denoted by $u_{\mathrm{Tx}}:\{0,P\}\times\{\hat{\epsilon},\check{\epsilon}\}^2\times\{\omega_{\mathrm{Tx}}^{(0)},\omega_{\mathrm{Tx}}^{(1)}\}\to\mathbb{R}$ and $u_{\mathrm{Rx}}:\{0,P\}^2\times\{\hat{\epsilon},\check{\epsilon}\}\times\{\omega_{\mathrm{Rx}}^{(0)},\omega_{\mathrm{Rx}}^{(1)}\}\to\mathbb{R}$. More specifically, the objective of the transmitter is to maximize the expectation of a given function u with respect to its individual beliefs. Such a function u models its aim to transmitting private information to the legitimate receivers. Conversely, the objective of the eavesdroppers is to minimize the expected value of the function u given its own individual beliefs. The function $u:\{0,\bar{P}\}\times\{\hat{\epsilon},\check{\epsilon}\}$ can be any function that is positive only when the transmitter sends information and the eavesdropper j^* is unable to extract any private information from its received signal $\boldsymbol{y}_{j^*}$, i.e., $P>0$ and $\mathrm{SNR}_{i*}>\mathrm{SNR}_{j*}+\epsilon$. Alternatively, u is negative when the transmitter sends information and the eavesdropper j^* is able to at least partially decode the private message, i.e., $P>0$, $\mathrm{SNR}_{i*}<\mathrm{SNR}_{j*}$ and $\mathrm{SNR}_{i*}>\mathrm{SNR}_{j*}+\epsilon$. Finally, u is zero when the transmitter sends information to the eavesdropper j^*, i.e., $P>0$ and $\mathrm{SNR}_{j^*}+\epsilon\geqslant\mathrm{SNR}_{i^*}$; or when the transmitter decides not to transmit, i.e., $\bar{P}=0$. One example for the function u is provided in [8], where

$$u\left(P,\epsilon\right)=\log\left(\frac{1+\mathrm{SNR}_{i^*}}{1+\mathrm{SNR}_{j^*}}\right)\mathbb{1}_{\left\{\mathrm{SNR}_{i^*}>\mathrm{SNR}_{j^*}+\epsilon\right\}}. \tag{8}$$

Therefore, the objective functions u_{Tx} and u_{Rx} are

$$u_{\mathrm{Tx}}(P,\boldsymbol{\epsilon},\omega_{\mathrm{Tx}})=\sum_{(a,b)\in\{A,\bar{A}\}\times\{B,\bar{B}\}}\Pr\left(a,b|\omega_{\mathrm{Tx}}\right)\left(u(P,\epsilon_0)+u(P,\epsilon_1)\right),\text{ and}$$
$$u_{\mathrm{Rx}}(\boldsymbol{P},\epsilon,\omega_{\mathrm{Rx}})=\sum_{(a,b)\in\{A,\bar{A}\}\times\{B,\bar{B}\}}\Pr\left(a,b|\omega_{\mathrm{Rx}}\right)\left(u(P_0,\epsilon)+u(P_1,\epsilon)\right),$$

respectively. The vector $\boldsymbol{\epsilon}=\left(\epsilon_0,\epsilon_1\right)$ is such that ϵ_0 and ϵ_1 are the error terms used by the eavesdropper Rx when it is at KS $\omega_{\mathrm{Rx}}^{(0)}$ (it does not know K) and KS $\omega_{\mathrm{Rx}}^{(1)}$ (it knows K), respectively. The vector $\boldsymbol{P}=\left(P_0,P_1\right)$ is such that P_0 and P_1 are the average powers at KS $\omega_{\mathrm{Tx}}^{(0)}$ (it does not know K and J) and KS $\omega_{\mathrm{Tx}}^{(1)}$ (it knows K and J), respectively. An interesting outcome of the game $\mathcal{G}$ is a Bayesian equilibrium (BE) [13]. At a BE, each player adopts an action for each of its possible knowledge states that is optimal with respect to the actions adopted by the other player at any of its knowledge states. Here, the optimality of the actions of one player is with respect to its individual beliefs. More formally, a BE can be defined as follows:

Definition 1 (Bayesian Equilibrium [13]): The action profiles $\boldsymbol{P}^*=(P_0^*,P_1^*)$ and $\boldsymbol{\epsilon}^*=\left(\epsilon_0^*,\epsilon_1^*\right)$ are a Bayesian equilibrium of the game $\mathcal{G}$, if $\forall(m,n)\in\{0,1\}^2$ and $\forall\boldsymbol{P}=\left(P_0,P_1\right)\in\{0,P\}^2$, it holds that

$$u_{\mathrm{Tx}}(P_n^*,\boldsymbol{\epsilon}^*,\omega_{\mathrm{Tx}}^{(n)})\quad\geqslant\quad u_{\mathrm{Tx}}(P_n,\boldsymbol{\epsilon}^*,\omega_{\mathrm{Tx}}^{(n)}), \tag{9}$$

and $\forall\boldsymbol{\epsilon}=\left(\epsilon_0,\epsilon_1\right)\in\{\hat{\epsilon},\check{\epsilon}\}^2$,

$$u_{\mathrm{Rx}}(\boldsymbol{P}^*,\epsilon_m^*,\omega_{\mathrm{Rx}}^{(m)})\quad\geqslant\quad u_{\mathrm{Rx}}(\boldsymbol{P}^*,\epsilon_m,\omega_{\mathrm{Rx}}^{(m)}). \tag{10}$$

The expected secrecy capacity and expected secrecy leakage observed at a BE is fully characterized in [8]. For the sake of completeness, these results are reproduced in Theorem 1, on the next page.

IV. Numerical Analysis

A. On the Impact of the Available Knowledge

From Theorem 1, for all $m\in\{0,1\}$ it follows that

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(m)},\omega_{\mathrm{Rx}}^{(0)})>\bar{C}_s(\omega_{\mathrm{Tx}}^{(m)},\omega_{\mathrm{Rx}}^{(1)}),\text{ and}$$
$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(m)},\omega_{\mathrm{Rx}}^{(0)})>\bar{L}_s(\omega_{\mathrm{Tx}}^{(m)},\omega_{\mathrm{Rx}}^{(1)})=0. \tag{11}$$

This implies that, independently of the knowledge available for the transmitter, providing more knowledge to the malicious receivers strongly decreases the secrecy capacity, which agrees with intuition. However, paradoxically, more knowledge also implies a zero information leakage rate. That is, no eavesdropping occurs when malicious receivers are more knowledgeable about the network. Indeed, more knowledge forces the eavesdroppers to preferably play $\hat{\epsilon}$. Hence, either a legitimate receiver is chosen as the destination and strictly positive secrecy rate is guaranteed ($\mathrm{SNR}_{k^*}>\mathrm{SNR}_{j^*}+\hat{\epsilon}$); or an eavesdropper is chosen as the destination ($\mathrm{SNR}_{j^*}+\hat{\epsilon}>\mathrm{SNR}_{k^*}$), which implies that no private information traverses the channel.

Theorem 1 (Secrecy Rate with Active Eavesdroppers): Let $\xi \in [0,1]$ and $1-\xi$ be the probabilities with which the eavesdroppers use their negative $\check{\epsilon}$ and positive $\hat{\epsilon}$ error terms, respectively. Let also $\bar{C}_s(\omega_{\mathrm{Tx}}^{(m)}, \omega_{\mathrm{Rx}}^{(n)})$ and $\bar{L}_s(\omega_{\mathrm{Tx}}^{(m)}, \omega_{\mathrm{Rx}}^{(n)})$ denote the expected secrecy capacity and the expected information leakage at the Bayesian equilibrium of the game $\mathcal{G}$ when the transmitter and the eavesdroppers have the knowledge state $\omega_{\mathrm{Tx}}^{(m)}$ and $\omega_{\mathrm{Rx}}^{(n)}$, with $(m,n) \in \{0,1\}^2$, respectively. Then,

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)}) = \xi \int_0^\infty \int_\alpha^\infty \log\left(\frac{1+\lambda P}{1+\alpha P}\right) \mathrm{d}F_{|h_{k^*}|^2}(\lambda) \mathrm{d}F_{|h_{j^*}|^2}(\alpha) + (1-\xi) \int_0^\infty \int_{\alpha+\frac{\check{\epsilon}}{P}}^\infty \log\left(\frac{1+\lambda P}{1+\alpha P}\right) \mathrm{d}F_{|h_{k^*}|^2}(\lambda) \mathrm{d}F_{|h_{j^*}|^2}(\alpha),$$

$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)}) = \xi \int_0^\infty \int_0^{\lambda - \frac{\check{\epsilon}}{P}} \log\left(1+\alpha P\right) \mathrm{d}F_{|h_{j^*}|^2}(\alpha) \mathrm{d}F_{|h_{k^*}|^2}(\lambda),$$

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(1)}) = \int_0^\infty \int_{\alpha+\frac{\check{\epsilon}}{P}}^\infty \log\left(\frac{1+\lambda P}{1+\alpha P}\right) \mathrm{d}F_{|h_{k^*}|^2}(\lambda) \mathrm{d}F_{|h_{j^*}|^2}(\alpha)$$

$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(1)}) = 0$$

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(0)}) = \begin{cases} \bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)}) & \textit{if } \Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}\right) > \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right) \\ 0 & \textit{otherwise} \end{cases}$$

$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(0)}) = \begin{cases} \bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)}) & \textit{if } \Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}\right) > \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right) \\ 0 & \textit{otherwise} \end{cases}$$

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(1)}) = \begin{cases} \bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(1)}) & \textit{if } \Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}\right) > \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right) \\ 0 & \textit{otherwise} \end{cases}$$

$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(1)}) = 0,$$

where i^* and k^* are defined by (4) *and* (5)*, respectively. The functions $F_{|h_{k^*}|^2}$ and $F_{|h_{j^*}|^2}$ are the respective cumulative probability distributions of the random variables $|h_{k^*}|^2$ and $|h_{j^*}|^2$.*

This explains the reduction of the secrecy capacity: legitimate transmitters become less likely to be chosen as destinations.

A similar counter-intuitive effect is observed at the transmitter. From Theorem 1, for all $n \in \{0,1\}$ it follows that,

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(n)}) > \bar{C}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(n)}), \text{ and} \tag{12}$$

$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(n)}) > \bar{L}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(n)}). \tag{13}$$

This implies that independently of the KS m of the malicious receivers, providing more knowledge to the transmitters reduces the expected secrecy capacity. This is observed because the transmitter becomes less willing to transmit. Bayesian inference implies that not transmitting any private information is safer depending on the number of legitimate and malicious receivers. Indeed, under the condition that $\Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}\right) < \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right)$, the transmitter does not transmit at all. This conservative behavior also explains the reduction in the information leakage rate, which is on the contrary a more intuitive observation.

B. On the Impact of the Signal to Noise Ratio

From Theorem 1, the following holds in the high SNR regime ($P \to \infty$), for all $(m,n) \in \{0,1\}^2$:

$$\lim_{P\to\infty} \bar{R}_s(\omega_{\mathrm{Tx}}^{(m)}, \omega_{\mathrm{Rx}}^{(n)}) = \xi \int_0^\infty \int_\alpha^\infty \log\left(\frac{\lambda}{\alpha}\right) \mathrm{d}F_{|h_{i^*}|^2}(\lambda) \mathrm{d}F_{|h_{j^*}|^2}(\alpha)$$

and

$$\lim_{P\to\infty} \bar{L}_s(\omega_{\mathrm{Tx}}^{(m)}, \omega_{\mathrm{Rx}}^{(n)}) = \xi \int_0^\infty \int_0^\lambda \log\left(1+\alpha P\right) \mathrm{d}F_{|h_{j^*}|^2}(\alpha) F_{|h_{i^*}|^2}(\lambda),$$

which implies that in the high SNR regime, independently of the available knowledge at the transmitter or receivers, a strictly positive secrecy capacity is guaranteed only if the malicious receivers use the negative error term $\check{\epsilon}$, at least a fraction $\xi > 0$ of all channel uses. The same is required for observing a strictly positive expected information leakage rate. This evokes the fact that the best performance for an active eavesdropper in the high SNR regime is to behave as a passive eavesdropper, i.e., avoiding to be chosen as the destination ($\xi = 1$). This coincides with the performance achieved at the Nash equilibrium when the transmitter and the receivers play with complete information [2].

C. On the Impact of the Additive Error $\hat{\epsilon}$ and $\check{\epsilon}$

When eavesdroppers ignore the number of legitimate receivers (KS $\omega_{\mathrm{Rx}}^{(0)}$), either a positive or negative additive error is indifferently used. This is basically because in expectation, both actions yield the same utility given their beliefs. Hence, if the probability of using a negative error term is denoted by ξ, it follows that $\xi \to 0$ implies that

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)}) \to \bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(1)}) \geqslant 0, \text{ and} \tag{14}$$

$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)}) \to \bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(1)}) = 0, \tag{15}$$

and moreover, $\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$ becomes monotonically decreasing with $\hat{\epsilon}$, as shown in Fig. 1 (top). That is, eavesdroppers would choose a large value of $\hat{\epsilon}$ in order to reduce the average secrecy capacity. Indeed, a sufficiently large value of $\hat{\epsilon}$ might reduce the secrecy capacity to zero. However, large values of $\hat{\epsilon}$ can also lead the transmitter to be suspicious about the malicious nature of the eavesdroppers and thus, be removed from the network. On the contrary, $\xi \to 1$ implies that $\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$ achieves a maximum that is independent of the value of $\hat{\epsilon}$ and, at the same time, $\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$ achieves a maximum that is dependent on $\check{\epsilon} < 0$. The smaller $\check{\epsilon}$, the larger is the leakage $\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$, as shown in Fig. 1 (bottom). This is basically because a small $\check{\epsilon}$ reduces the likelihood of a malicious receiver to be chosen as the destination and thus, more private information crosses the wireless channel, thereby increasing the possibility of eavesdropping.

Finally, it is worth highlighting that when eavesdroppers know the value of K (KS $\omega_{\mathrm{Rx}}^{(1)}$), they do not use the negative error term at all, as the Bayesian inference induces the beliefs that their individual SNRs are most likely lower than the highest SNR of the legitimate receivers. Therefore, malicious receivers always play $\hat{\epsilon}$ to prohibit the transmitter from choosing legitimate receivers as the destination.

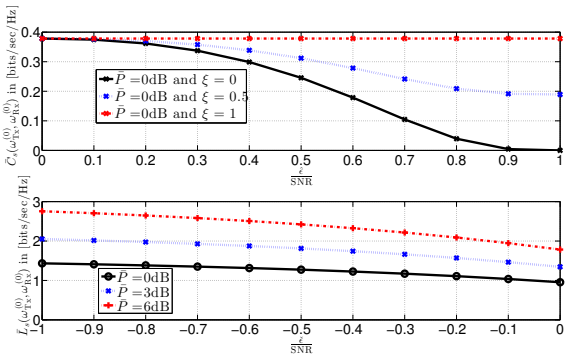

Fig. 1. Average secrecy capacity $\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$ (Top) and average leakage $\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$ (Bottom) as a function of $\frac{\hat{\epsilon}}{\mathrm{SNR}_{j^*}}$, with $K = J = 5$ and j^* given by (5).

D. On the Impact of the Number of Legitimate Users and Eavesdroppers

From Theorem 1, it can be concluded that when the transmitter knows the number of eavesdroppers (KS $\omega_{\mathrm{Tx}}^{(1)}$), its transmission ($\bar{P} > 0$) is subject to the satisfaction of the condition

$$\Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}\right) > \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right). \tag{16}$$

Condition (16) verifies whether the probability of sending information with a strictly positive secrecy rate to a legitimate destination ($\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}$) is higher than the probability of sending private information to a legitimate destination when a strictly positive secrecy rate is unfeasible and the eavesdropper with the highest SNR j^* is able to trick the transmitter by reporting a degraded SNR ($\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}$). That is, condition (16) verifies whether the utility function of the transmitter in the corresponding game in [8] is strictly positive while playing $\bar{P} = P > 0$, given its own beliefs. It is important to highlight that if $\check{\epsilon}$ can be written as a fraction of the SNR_{j^*}, condition (16) is independent of the transmit power and depends only on the value of $\check{\epsilon}$, the number of legitimate transmitters K and eavesdroppers J, as the expectation is taken over the distributions of the channel realizations h_{i^*} and h_{j^*}. Fig. 4 plots $\Delta(K, J) = \Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}\right) - \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right)$ as a function of the number of eavesdroppers J and the number of legitimate users K, when $\check{\epsilon} = \frac{1}{2}\mathrm{SNR}_{j^*}$. Note that (16) is satisfied, i.e., $\Delta(K, J) > 0$, when the number of eavesdroppers J and legitimate users K satisfy the condition

$$K \geqslant \max\left(1, J - 3\right), \tag{17}$$

for this particular value of $\check{\epsilon} = \frac{1}{2}\mathrm{SNR}_{j^*}$. Hence, when the number of legitimate transmitters exceeds by three the number of eavesdroppers, the transmitter sends information to destination i^*, which guarantees positive secrecy capacity on average. This also verifies that condition (16) can be evaluated by the transmitter at the KS $\omega_{\mathrm{Tx}}^{(1)}$ as it depends on parameters whose values are known at such knowledge state.

Interestingly, note that when the SNR is arbitrarily increased

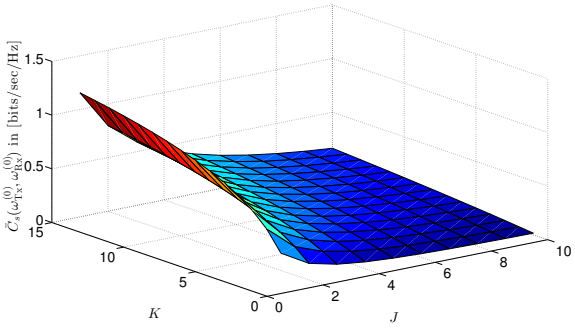

Fig. 2. Average secrecy capacity $\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$ as a function of the number of eavesdroppers J and the number of legitimate users K, when $P = 0$ dB, $\xi = 0$ and $\hat{\epsilon} = \frac{1}{2}\mathrm{SNR}_{j^*}$.

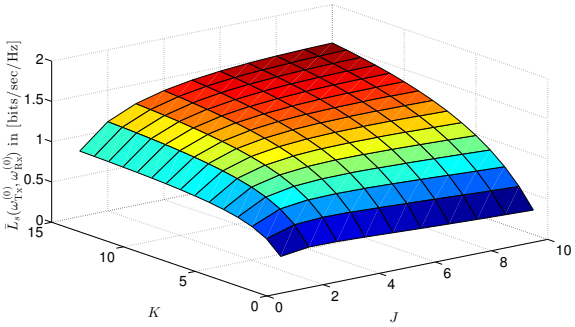

Fig. 3. Average leakage $\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(0)})$ as a function of the number of eavesdroppers J and the number of legitimate users K, when $P = 0$ dB, $\xi = 1$ and $\hat{\epsilon} = \frac{1}{2}\mathrm{SNR}_{j^*}$.

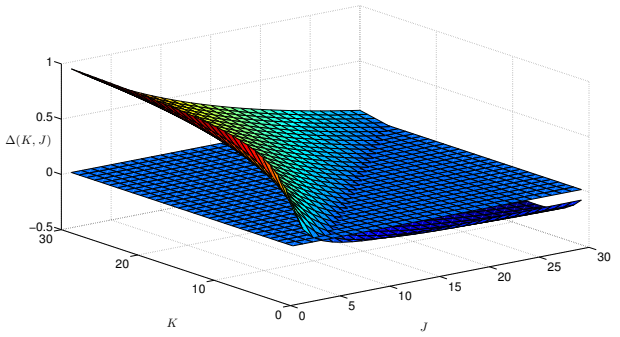

Fig. 4. $\Delta(K, J)$ as a function of the number of eavesdroppers J and the number of legitimate users K, with $\Delta(K, J) = \Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{k^*}\right) - \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{k^*} < \mathrm{SNR}_{j^*}\right)$ and $\check{\epsilon} = \frac{1}{2}\mathrm{SNR}_{j^*}$.

while the error term $\check{\epsilon}$ is kept constant, condition (16) is always satisfied. Hence, in the high SNR regime ($P \to \infty$), the transmitter is always able to transmit at a positive secrecy rate. Nonetheless, if the error terms are both dynamically adjusted by the eavesdroppers according to their actual SNRs, increasing the SNR does not provide any additional robustness against the actions of the eavesdroppers.

When the transmitter decides to send information to receiver i^*, either because it is at knowledge state $\omega_{\mathrm{Tx}}^{(0)}$ or because it is at knowledge state $\omega_{\mathrm{Tx}}^{(1)}$ and condition (16) is satisfied, the average secrecy rate is always strictly positive. As shown in Fig. 2, the average secrecy capacity increases monotonically with the number of legitimate receivers. This is due to the fact that a higher number of legitimate transmitters increases the likelihood of choosing a legitimate transmitter $i^* \in \mathcal{K}$ as the destination and ensuring a strictly positive secrecy rate ($\mathrm{SNR}_{j^*} < \mathrm{SNR}_{k^*}$). Alternatively, increasing the number of eavesdroppers increases the probability that an eavesdropper will be chosen as the destination, which avoids the transmission of private information. This is the reason why the average secrecy capacity decreases with $\hat{\epsilon}$ and is independent of $\check{\epsilon}$.

Conversely to the average secrecy capacity, the information leakage increases with both the number of legitimate transmitters and eavesdroppers. This is because $K \to \infty$ increases the probability of choosing a legitimate receiver as the destination, and thus private information traverses the channel more frequently. Moreover, $J \to \infty$ increases the average SNR of eavesdropper j^*, and thus it is able to extract more information from the channel. This explains why the average leakage depends on ξ and $\check{\epsilon}$ and is independent of $\hat{\epsilon}$.

V. Conclusions

This paper has revisited previous results on the tradeoffs between network-state knowledge and the feasibility of secrecy [8]. Using such results, a numerical analysis has been presented to highlight the different behaviors induced by different individual states at which particular global knowledge about the network is available. Special attention has been paid to the impact of the ability of eavesdroppers to report degraded or improved values of their SNRs on the average secrecy rate and average information leakage. At each knowledge state, both the eavesdroppers and the transmitter exhibit significantly different behaviors, indeed, some of them might appear paradoxical. In particular, letting eavesdroppers know the number of legitimate receivers and the total number of eavesdroppers induces a conservative behavior that makes them less harmful in terms of average information leakage. Similarly, letting the transmitter know the number of active eavesdroppers induces a more careful behavior in which it is less willing to transmit, which reduces the expected secrecy capacity.

References

[1] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "Physical layer security in wireless networks with passive and active eavesdroppers," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, Anaheim, CA, Dec. 2012.

[2] A. Chorti, S. M. Perlaza, H. V. Poor, and Z. Han, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE Journal on Selected Areas in Communications, Special Issue on Signal Processing Techniques for Wireless Physical Layer Security*, to appear.

[3] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[4] V. Aggarwal, L. Lai, A. R. Calderbank, and H. V. Poor, "Wiretap channel II with an active eavesdropper," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, Jun. 2009.

[5] S. Shafiee and S. Ulukus, "Mutual information games in multiuser channels with correlated jamming," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4598–4607, Oct. 2009.

[6] A. Mukherjee and A. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[7] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[8] S. M. Perlaza, A. Chorti, H. V. Poor, and Z. Han, "On the impact of network-state knowledge on the feasibility of secrecy," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, Jul. 2013.

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

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

[11] E. T. Jaynes, "Information theory and statistical mechanics," *Physical Review*, vol. 106, no. 4, pp. 620–630, May 1957.

[12] J. Harsanyi, "Games with incomplete information played by Bayesian players. Part I: The basic model," *Management Science*, vol. 14, no. 3, pp. 159–182, Nov. 1967.

[13] ——, "Games with incomplete information played by Bayesian players. Part II: Bayesian equilibrium points," *Management Science*, vol. 14, no. 5, pp. 320–334, Jan. 1968.