On the impact of network-state knowledge on the Feasibility of secrecy

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

On the Impact of Network-State Knowledge on the Feasibility of Secrecy

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

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

***Abstract*—In this paper, the impact of network-state knowledge is studied in the context of decentralized active non-colluding eavesdropping. The main contribution is a formal proof of a paradoxical effect that might appear when increasing the available knowledge at each of the network components. Using a broadcast channel similar to the time-division downlink of a single-cell cellular system, it is shown that providing more knowledge to both the transmitter and the receivers negatively affects their performance. Eavesdroppers become more conservative in their attacks, which makes them harmless in terms of information leakage, whereas the transmitter becomes more careful and less willing to transmit, which reduces the expected secrecy capacity of this channel. Finally, it is shown that this counter-intuitive effect vanishes in the high SNR regime, in which the system becomes resilient to active attacks.**

I. Introduction

In the presence of adversarial or untrustworthy receivers, physical-layer security is a paradigm that exploits the properties of the channel to ensure secrecy in the transmission of information. Starting with the seminal work of Shannon [1], information theorists have focused on the extraction of private information from the simple observation of the signals traversing the channel, e.g., passive eavesdropping upon wireless or fiber-optical channels. However, under the risk of being detected, malicious components can interact with their legitimate counterparts and intensify the information leakage or damage to the network, e.g., impersonation or active eavesdropping. In the majority of existing studies, the underlying strategy in active attacks relies on sending jamming signals to degrade the communications. Malicious components use jamming to reduce the secrecy rate and legitimate components use it to degrade the signals observed by the eavesdroppers [2]–[6].

In this paper, active eavesdropping is studied from the perspective of false signaling and the relevance of network-state knowledge in each of the network components is highlighted. For this purpose, the scenario under analysis is a broadcast channel similar to a time-division downlink of a single-cell cellular system in which the destination is chosen as the receiver with the highest reported signal-to-noise ratio (SNR). Malicious receivers, which are assumed to be non-colluding, report false SNR aiming to mislead the destination selection whereas the transmitter chooses whether to transmit or not. Reporting an SNR higher than the actual value makes a malicious receiver more likely to be chosen as the destination and prohibits the transmitter from sending private information to legitimate receivers. In contrast, reporting a lower SNR forces the transmitter to choose another receiver as the destination, possibly a legitimate receiver, that is more susceptible to eavesdropping. The analysis of this scenario is performed using tools from Bayesian inference and game theory. The main conclusions are surprisingly counter-intuitive and reveal that the feasibility of eavesdropping in decentralized systems depends on the knowledge available at each of the network components. In particular, it is shown that, unlike a completely ignorant eavesdropper, an eavesdropper that knows the number of legitimate receivers "plays more conservatively". For instance, it tends to report a higher SNR which decreases the leakage rate as less private information is traversing the channel. In parallel, compared to a completely ignorant transmitter, a transmitter that knows the number of legitimate and malicious receivers becomes less willing to broadcast private messages; as a result, the average secrecy rate decreases. Hence, this simple example shows that in decentralized systems, more knowledge does not necessarily render the attacker more harmful or the defender more powerful.

The paper is organized as follows: the problem formulation is outlined in Section II. Section III includes the Bayesian game theoretic analysis, while the main results and discussion are included in Section IV. Due to space limitations, the proofs of the main results are omitted and this paper is constrained only to the presentation and discussion of these results.

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 non-colluding 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 channel use, for all $i \in \mathcal{D}$, the message index $m_i \in \mathcal{M}_i$ is encoded to 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 $\mathbb{E}\left[\boldsymbol{x}_i^2\right] \leqslant \bar{P}$, with $\bar{P}$ the average transmit power. The input to receiver i during a given channel

This research was supported in part by the U. S. Army Research Office under MURI Grant W911NF-11-1-0036, and in part by the IOF APLOE (PIOF-GA-2010-274723) grant within the 7th Framework Program of the European Community.

use 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 $\boldsymbol{z}_i = (z_{i,1}, \ldots, z_{i,N_i})$ is such that the components $z_{i,1}, \ldots, z_{i,N_i}$ as well as the channel coefficients $h_1, \ldots, h_{K+J}$ are 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:

$$\begin{aligned} C_s(k,j) &= \max_{\mathbb{E}\left[\boldsymbol{X}_k^2\right] < \bar{P}} I(\boldsymbol{X}_k; \boldsymbol{Y}_k) - I(\boldsymbol{X}_k; \boldsymbol{Y}_j) \\ &= \Big(\log(1+\mathrm{SNR}_k) - \log(1+\mathrm{SNR}_j)\Big)^+, \end{aligned} \tag{2}$$

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

$$L_s(k,j) \quad = \quad \max_{\mathbb{E}\left[\boldsymbol{X}_k^2\right] < \bar{P}} I(\boldsymbol{X}_k; \boldsymbol{Y}_j) = \log(1+\mathrm{SNR}_j).$$

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 $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_{K+J})$, where γ_i denotes the SNR reported by receiver i. Then, the index i^* is such that

$$i^* = \arg\max_{i \in \mathcal{D}} \gamma_i. \tag{3}$$

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 [7]:

$$j^* = \arg\max_{j \in \mathcal{J}} \gamma_j. \tag{4}$$

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, malicious 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 both $\hat{\epsilon}$ and $\check{\epsilon}$ are autonomously determined by the eavesdroppers and no restriction is imposed over the exact value. For instance, when SNR_j is the highest SNR in the network ($j = i^*$), eavesdropper j can eavesdrop upon all legitimate receivers, as long as it is able to forge the transmitter and make it choose a legitimate receiver as the destination during that time interval. Hence, malicious receiver j reports a lower SNR $\gamma_j = \mathrm{SNR}_j + \check{\epsilon}$, such that $j^* \neq \arg\max_{i \in \mathcal{D}} \gamma_i$. In this way, it forces the transmitter to send private information to another receiver susceptible to eavesdropping. Alternatively, if SNR_j is not the highest SNR ($j \neq i^*$), then the interest of malicious receiver j is to be selected as the destination such that no private information is sent to legitimate 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 private 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. A : Eavesdropper j^* is able to eavesdrop, i.e., $\mathrm{SNR}_{j^*} > \mathrm{SNR}_{i^*}$; and B : Eavesdropper j^* is able to trick the transmitter, that is, to make the transmitter choose receiver j^* as the destination when $j^* \neq i^*$, i.e.,

$$\hat{\epsilon} > \left|\mathrm{SNR}_{i^*} - \mathrm{SNR}_j^*\right|, \tag{5}$$

and to make the transmitter choose a destination different from j^* when $j^* = i^*$ i.e.,

$$\check{\epsilon} < -\left|\left(\mathrm{SNR}_{i^*} - \mathrm{SNR}_j^*\right)\right|. \tag{6}$$

The feasibility of eavesdropping depends on the events A and B. In state (A, B) eavesdropping is feasible but might not necessarily occur, as it depends on the choices of the transmitter and receiver j^*. In state $(A, \bar{B})$, eavesdropper j^* is chosen as the destination. In $(\bar{A}, B)$, the eavesdropper j^* can at most mislead the destination selection but cannot eavesdrop. In the state $(\bar{A}, \bar{B})$, a legitimate destination is always selected and strictly positive secrecy rate can be guaranteed.

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 it possesses estimates of the values of $\hat{\epsilon}$ and $\check{\epsilon}$ using standard tools [8]. 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 $\epsilon = \check{\epsilon}$. Note also that the estimates available at the transmitter might or might not be exact with respect to the actual values $\hat{\epsilon}$ or $\check{\epsilon}$ used by the eavesdroppers. 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 [9], 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

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

where j^* is defined by (4) and

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

The probability is taken over 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. Thus, there is no other knowledge available to make a better guess about the network state than a uniform probability distribution [9]. 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. Thus, 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 (4) and (7), respectively. The probability is taken over 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. Game Theoretic Analysis

The interaction between the transmitter and the malicious receivers during a sufficiently large number of independent channel uses can be modeled by a Bayesian game [10]. As we shall see, an interesting outcome of this game would be a Bayesian equilibrium [10], which models the lack of knowledge of all the network components.

A. A Bayesian Game

Consider a Bayesian game of the form: $\mathcal{G}=\left(\mathcal{P},\{\mathcal{A}_i\}_{i\in\mathcal{P}},\mathcal{S},\{\Omega_i\}_{i\in\mathcal{P}},\{\mathcal{B}_i\}_{i\in\mathcal{P}},\{u_i\}_{i\in\mathcal{P}}\right)$. The following describes each of these components. The set of players $\mathcal{P}=\{\mathrm{Tx},\mathrm{Rx}\}$ includes the transmitter (Tx) and the malicious receiver j^* (Rx) in (4). Note that even though there are several eavesdroppers, the secrecy capacity (2) and the information leakage (3) are calculated with respect to the eavesdropper j^*. Neither the other eavesdroppers nor the legitimate transmitters are considered part of the game. Indeed, their decisions do not impact the outcome of the game. However, note that i^* and j^* take different values at each channel use. This explains why the random variables $|h_{i^*}|^2$ and $|h_{j^*}|^2$ are both order statistics. The game is played as follows. At each channel use, the transmitter Tx chooses whether to transmit ($\bar{P}=P>0$) or not ($\bar{P}=0$) to destination i^*. The malicious receiver chooses either a positive $\hat{\epsilon}$ or negative $\check{\epsilon}$ additive error. Therefore, $\mathcal{A}_{\mathrm{Tx}}=\{0,P\}$ and $\mathcal{A}_{\mathrm{Rx}}=\{\hat{\epsilon},\check{\epsilon}\}$. The game can be played in any of the states in the set $\mathcal{S}$ of network states, $\mathcal{S}=\left\{(a,b)\in\{A,\bar{A}\}\times\{B,\bar{B}\}\right\}$, as described in Sec. II-C. However, none of the players knows exactly the actual state of the game at each channel use. Their partial knowledge about the network is given in terms of the knowledge states in the sets Ω_{Tx} and Ω_{Rx} for players Tx and Rx respectively. Therefore, $\Omega_{\mathrm{Tx}}=\{\omega_{\mathrm{Tx}}^{(0)},\omega_{\mathrm{Tx}}^{(1)}\}$ and $\Omega_{\mathrm{Rx}}=\{\omega_{\mathrm{Rx}}^{(0)},\omega_{\mathrm{Rx}}^{(1)}\}$. For each knowledge state, players have different beliefs about the actual state of the network. These beliefs are described in terms of the probabilities $\Pr\left(\boldsymbol{S}|\omega_{\mathrm{Tx}}^{(m)}\right)$ and $\Pr\left(\boldsymbol{S}|\omega_{\mathrm{Rx}}^{(m)}\right)$, for all $\boldsymbol{S}\in\mathcal{S}$ and for all $m\in\{0,1\}$. Therefore, the sets of beliefs $\mathcal{B}_{\mathrm{Tx}}$ and $\mathcal{B}_{\mathrm{Rx}}$ are $\mathcal{B}_{\mathrm{Tx}}=\{\Pr(\boldsymbol{S}|\omega_{\mathrm{Tx}}):\boldsymbol{S}\in\mathcal{S},\ \omega_{\mathrm{Tx}}\in\Omega_{\mathrm{Tx}}\}$, $\mathcal{B}_{\mathrm{Rx}}=\{\Pr(\boldsymbol{S}|\omega_{\mathrm{Rx}}):\boldsymbol{S}\in\mathcal{S},\ \omega_{\mathrm{Rx}}\in\Omega_{\mathrm{Rx}}\}$.

The interests of Tx and Rx are modeled by the function $u:\mathcal{A}_{\mathrm{Tx}}\times\mathcal{A}_{\mathrm{Rx}}\to\mathbb{R}$, given by

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

Note that the values of the function u depend not only on the actions $\bar{P}$ and ϵ but also on the exact realization of the channel gains h_{i^*} and h_{j^*}, via SNR_{i^*} and SNR_{j^*}. Thus, none of the players can determine the value of u at a given channel use, which is fundamental to determining the optimal actions. For instance, u 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., $\bar{P}>0$ 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., $\bar{P}>0$, $\mathrm{SNR}_{i*}<\mathrm{SNR}_{j*}$ and $\mathrm{SNR}_{i*}>\mathrm{SNR}_{j*}+\epsilon$. Finally, u is zero when the transmitter sends information to the eavesdropper j^*, i.e., $\bar{P}>0$ and $\mathrm{SNR}_{j^*}+\epsilon\geqslant\mathrm{SNR}_{i^*}$; or when the transmitter decides not to transmit, i.e., $\bar{P}=0$.

From this perspective and from the assumption that the transmitter has only a binary choice, player Tx aims to maximize the function u by choosing $\bar{P}\in\{0,P\}$, while the eavesdropper aims to minimize it by choosing $\epsilon\in\{\hat{\epsilon},\check{\epsilon}\}$. Note that the eavesdropper has an infinite number of choices given the conditions $\hat{\epsilon}>0$ and $\check{\epsilon}<0$. However, given that the value of the utility function depends only on whether $\hat{\epsilon}$ and $\check{\epsilon}$ satisfy (5) and (6), respectively, there is no loss of generality by considering the set $\boldsymbol{A}_{\mathrm{Rx}}$ as binary with $\hat{\epsilon}$ and $\check{\epsilon}$ fixed and chosen to satisfy (5) and (6). If the values $\hat{\epsilon}$ and $\check{\epsilon}$ do not satisfy these conditions, the behavior of the eavesdroppers does not affect the utility of the transmitter.

Finally, due to the lack of information, these optimizations are done over the expected value of the function u given each player's beliefs about the unknown parameters of the network. These objectives are denoted by $u_{\mathrm{Tx}}:\mathcal{A}_{\mathrm{Tx}}\times\mathcal{A}_{\mathrm{Rx}}^{|\Omega_{\mathrm{Rx}}|}\times\Omega_{\mathrm{Tx}}\to$

$\mathbb{R}$ and $u_{\mathrm{Rx}} : \mathcal{A}_{\mathrm{Tx}}^{|\Omega_{\mathrm{Tx}}|} \times \mathcal{A}_{\mathrm{Rx}} \times \Omega_{\mathrm{Rx}} \to \mathbb{R}$. Then, the expected value of u given the beliefs of Tx and Rx are

$$u_{\mathrm{Tx}}(P, \boldsymbol{\epsilon}, \omega_{\mathrm{Tx}}) = \sum_{m=0}^{|\Omega_{\mathrm{Rx}}|-1} \sum_{S \in \mathcal{S}} \Pr\left(S|\omega_{\mathrm{Tx}}\right) u(P, \epsilon_m), \text{ and}$$

$$u_{\mathrm{Rx}}(\boldsymbol{P}, \epsilon, \omega_{\mathrm{Rx}}) = \sum_{m=0}^{|\Omega_{\mathrm{Tx}}|-1} \sum_{S \in \mathcal{S}} \Pr\left(S|\omega_{\mathrm{Rx}}\right) u(P_m, \epsilon),$$

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 $\bar{\boldsymbol{P}} = \left(\bar{P}_0, \bar{P}_1\right)$ is such that $\bar{P}_0$ and $\bar{P}_1$ 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 the Bayesian equilibrium (BE). At the 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 is with respect to the individual beliefs. More formally, a BE can be defined as follows:

Definition 1 (Bayesian Equilibrium [10]): 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 $\forall \boldsymbol{P} = \left(P_0, P_1\right) \in \mathcal{A}_{\mathrm{Tx}}^2$, it holds that

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

and $\forall \boldsymbol{\epsilon} = \left(\epsilon_0, \epsilon_1\right) \in \mathcal{A}_{\mathrm{Rx}}^{|\Omega_{\mathrm{Rx}}|}$,

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

The following describes the average secrecy capacity and the average information leakage (Theorem 1) at the Bayesian equilibrium of the game $\mathcal{G}$.

IV. Main Results

The main result of this paper is presented in Theorem 1 at the top of the next page. Theorem 1 provides expressions for the expected secrecy capacity and the expected information leakage of the network at the BE. Before introducing the main result, the following subsection describes the BE of the game $\mathcal{G}$ and later, the main conclusions from Theorem 1 are presented.

A. Bayesian Equilibrium

The equilibrium (Def. 1) of the game $\mathcal{G}$ is described by the following lemma.

Lemma 1 (Bayesian Equilibria of $\mathcal{G}$): The action profiles $((P, P), (\hat{\epsilon}, \hat{\epsilon}))$ and $((P, P), (\check{\epsilon}, \hat{\epsilon}))$ are both BEs of the game $\mathcal{G}$ if the following holds:

$$\Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{i^*}\right) > \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{i^*} < \mathrm{SNR}_{j^*}\right),$$

where the probability is taken over the distribution of the random variables $|h_{i^*}|^2$ and $|h_{j^*}|^2$. Otherwise, the BE action profiles are $((P, 0), (\hat{\epsilon}, \hat{\epsilon}))$ and $((P, 0), (\check{\epsilon}, \hat{\epsilon}))$.

At the equilibrium, if the transmitter ignores the number of malicious receivers (KS $\omega_{\mathrm{Tx}}^{(0)}$), then it always sends information to destination i^*. This is basically because Bayesian inference implies that

$$u_{\mathrm{Tx}}\left(0, \boldsymbol{\epsilon}, \omega_{\mathrm{Tx}}^{(0)}\right) \leqslant u_{\mathrm{Tx}}\left(P, \boldsymbol{\epsilon}, \omega_{\mathrm{Tx}}^{(0)}\right), \tag{11}$$

for all $\boldsymbol{\epsilon} \in \mathcal{A}_{\mathrm{Rx}}^2$ and $P > 0$. Alternatively, when the transmitter knows the value of J (KS $\omega_{\mathrm{Tx}}^{(1)}$), it is able to determine whether transmitting at a positive secrecy rate is more likely than transmitting with a strictly positive information leakage rate. Therefore, the choice of sending information or not is conditioned on the number of legitimate and malicious receivers as well as the estimates of the error terms $\hat{\epsilon}$ and $\check{\epsilon}$. When eavesdroppers ignore the number of legitimate receivers (KS $\omega_{\mathrm{Rx}}^{(0)}$), they indifferently use either a positive or negative additive error as $u_{\mathrm{Rx}}\left(\boldsymbol{P}, \hat{\epsilon}, \omega_{\mathrm{Rx}}^{(0)}\right) = u_{\mathrm{Rx}}\left(\boldsymbol{P}, \check{\epsilon}, \omega_{\mathrm{Rx}}^{(0)}\right)$, for all $\boldsymbol{P} \in \mathcal{A}_{\mathrm{Tx}}^2$. When they 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 play $\hat{\epsilon}$ to prohibit the transmitter from choosing legitimate receivers as the destination.

Lemma 1 shows that the behavior of the transmitter and the active eavesdroppers is strongly dependent on their available knowledge. In the following, Lemma 1 is used to interpret some counter-intuitive observations derived from Theorem 1.

B. On the Impact of Available Knowledge

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

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

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 ($\mathrm{SNR}_{i^*} > \mathrm{SNR}_{j^*} + \hat{\epsilon}$); or an eavesdropper is chosen as the destination ($\mathrm{SNR}_{j^*} + \hat{\epsilon} > \mathrm{SNR}_{i^*}$), which implies that no private information traverses the channel. This also 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 $m \in \{0, 1\}$ it follows that,

$$\bar{C}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(m)}) > \bar{C}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(m)}), \text{ and} \tag{13}$$
$$\bar{L}_s(\omega_{\mathrm{Tx}}^{(0)}, \omega_{\mathrm{Rx}}^{(m)}) > \bar{L}_s(\omega_{\mathrm{Tx}}^{(1)}, \omega_{\mathrm{Rx}}^{(m)}). \tag{14}$$

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 $\Pr\left(\mathrm{SNR}_{j^*} \leqslant \mathrm{SNR}_{i^*}\right) < \Pr\left(\mathrm{SNR}_{j^*} + \check{\epsilon} \leqslant \mathrm{SNR}_{i^*} < \mathrm{SNR}_{j^*}\right)$, the transmitter does not transmit at all. This more conservative behavior also explains the reduction in the information leakage rate, which is on the contrary a more intuitive observation.

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,

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

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

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

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

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

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

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

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

where i^* and k^* are defined by (3) *and* (4)*, 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 $|h_{j^*}|^2$.*

C. High SNR Regime

In the high SNR regime ($P \to \infty$), the following holds from Theorem 1, 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 [7].

V. Conclusions

This paper has shown that in the context of active eavesdropping, a paradoxical effect might appear when increasing the available knowledge at each network component. In the particular scenario considered in this paper, additional knowledge by the eavesdroppers induces conservative behavior that makes them harmless in terms of the expected information leakage. Similarly, more knowledge by the transmitter makes it more careful and less willing to transmit in order to avoid eavesdropping, which reduces the expected secrecy capacity. These observations highlight the relevance of the available knowledge at each network component when studying secrecy with active eavesdropping in decentralized systems.

References

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

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