ISIT'2013 1569719757

To Obtain or not to Obtain CSI in the Presence of Hybrid Adversary

Y. Ozan Basciftci
Dep. of Electrical & Computer Eng.
The Ohio State University
Columbus, Ohio, USA
Email: basciftci.1@osu.edu

C. Emre Koksal
Dep. of Electrical & Computer Eng.
The Ohio State University
Columbus, Ohio, USA
Email: koksal@ece.osu.edu

Fusun Ozguner
Dep. of Electrical & Computer Eng.
The Ohio State University
Columbus, Ohio, USA
Email: ozguner@ece.osu.edu

***Abstract*—We consider the wiretap channel model under the presence of a hybrid, half duplex adversary that is capable of either jamming or eavesdropping at a given time. We analyzed the achievable rates under a variety of scenarios involving different methods for obtaining transmitter CSI. Each method provides a different grade of information, not only to the transmitter on the main channel, but also to the adversary on all channels. Our analysis shows that main CSI is more valuable for the adversary than the jamming CSI in delay-limited scenarios. Similarly, in certain cases under the ergodic scenario, interestingly, no CSI may lead to higher achievable secrecy rates than with CSI.**

I. Introduction

Information theoretic security has received a significant attention recently. One mainstream direction has been on the wireless transmission of confidential messages from a source to a destination, in the presence of internal and/or external eavesdroppers. Toward achieving that goal, the communicating pair exploits the stochasticity and the asymmetry of wireless channels between the communicating pair and the eavesdroppers. A stochastic encoder at the transmitter makes use of the available channel state information (CSI) in a way for the mutual information leaked to the adversaries remain arbitrarily small. It is designed in a way that, even when the adversaries have access to the full CSI of the main channel, i.e., between the transmitter and the receiver as well as the eavesdropper channel, i.e., between the transmitter and itself, it still will obtain an arbitrarily low rate of information on the message. Likewise, the adversary relies on CSI to make decisions. For instance, a half-duplex hybrid adversary, capable of jamming or eavesdropping at a given time (but not both simultaneously) decides between jamming vs. eavesdropping, based on the available CSI.

The assumption that the adversaries have full CSI of all channels is typical in the literature [1]-[3]. While this assumption leads to robust systems in terms of providing security as it makes no assumptions on the adversaries, it can be too conservative in some cases. For example, to obtain main CSI, an adversary relies on the same resource as the transmitter: feedback from the legitimate receiver. Hence, from the perspective of the receiver, there is a tradeoff between revealing CSI and keeping it secret.

To that end, we focus on the system depicted in Figure 1. We assume all three channels to be block fading. In each block, based on the available CSI, the half-duplex adversary can choose to do jamming at a fixed transmission power or eavesdropping, but not both. Our objective is to maximize the rate of reliable communication over the main channel, subject to full equivocation [4] (weak secrecy) at the adversary. The adversary can follow an arbitrary strategy in its choice of jamming vs. eavesdropping at any given block. Consequently, the system reduces to the *arbitrarily varying wiretap channel*. We investigate the achievable rates and associated strategies for the legitimate users under a variety of scenarios involving the available CSI.

In the case in which the receiver feeds back main CSI, it may do so in two ways: directly by sending back the exact state of the channel or by sending reverse pilots, trying to exploit channel reciprocity (similar to [5]). While the former method completely reveals the main CSI, it eliminates the possibility of the adversary to learn the jammer CSI. On the other hand, while the pilot feedback successfully hides the main CSI, it enables the adversary to estimate the jammer CSI. In terms of the secrecy encoding strategies, we address the possibilities under two general scenarios: the ergodic and the delay-limited. In the former case, one message is encoded across infinitely many blocks and in the latter case, a separate message is encoded over each block, to be decoded immediately. Thus, in the delay-limited scenario, we also impose an additional probabilistic constraint on the decoding and secrecy outage events.

In the delay limited scenario, we show that by revealing the main CSI, the receiver achieves a higher secrecy rate under the outage constraint, compared to transmission with no CSI. Furthermore, we show that main CSI is more valuable for the adversary than the jamming CSI in both delay-limited. In the ergodic scenario, we observe that the transmitter may not need the CSI to achieve higher secrecy rates.

There is a recent research interest on hybrid adversaris. In [7], the authors formulate the MIMO wiretap channel as a two player zero-sum game in which the payoff function is an achievable ergodic secrecy rate. The strategy of the

This work is supported in part by QNRF under grant NPRP 5-559-2-227, and by NSF under grants CNS-1054738, CNS-0831919, CCF-0916664, and ECCS-0931669.

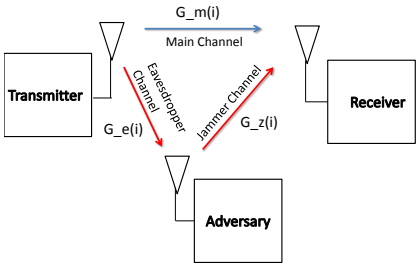


Fig. 1. System Model

transmitter is to send the message in a full power or to utilize some of the available power to produce artificial noise. The conditions under which pure Nash equilibrium exists are studied. In [6], the authors consider fast fading main and eavesdropper channels and static jammer channel. Under this channel configuration, they propose a novel encoding scheme which is called block-Markov Wyner secrey encoding. In [8], the authors introduce a pilot contamination attack in which the adversary jams during the reverse training phase to prevent the transmitter from estimating the main CSI correctly. As a result, the transmitter incorrectly designs precoder which will increase the signal strength at the adversary that eavesdrops the main channel during the data transmission phase.

The rest of this paper is organized as follows. In Section II, we first describe the system model. We then explain the channel model and CSI feedback models. At the end of the section, we explain the problem formulations. In Section III, we present the results for both delay limited and ergodic scenarios. In Section V, we present our numerical results and conclude the paper in Section VI.

II. System Model and Problem Formulation

A. Channel Model

In this paper, we focus on a block fading channel model. Time is divided into discrete blocks and there are N channel uses in each block. Channel state is assumed to be constant within a block and varies randomly from one block to the next. We assume all parties are half-duplex, thus the adversary can not jam and eavesdrop simultaneously.

The observed signals at the legitimate receiver and the adversary in i-th block are as follows:

$$Y^N(i) = G_m(i)x^N(i) + G_z(i)S_j^N(i)\phi(i) + S_m^N(i) \quad (1)$$

$$Z^N(i) = \begin{cases} G_e(i)x^N(i) + S_e^N(i) & \text{if } \phi(i) = 0 \\ \emptyset & \text{if } \phi(i) = 1 \end{cases} \quad (2)$$

where $x^N(i)$ is the transmitted signal, $Y^N(i)$ is the signal received by the legitimate receiver, $Z^N(i)$ is the signal received by the adversary, $S_j^N(i)$, $S_m^N(i)$, and $S_e^N(i)$ are noise vectors distributed as complex Gaussian, $\mathcal{CN}(\mathbf{0}, P_j I_{N\times N})$, $\mathcal{CN}(\mathbf{0}, I_{N\times N})$, and $\mathcal{CN}(\mathbf{0}, I_{N\times N})$, respectively, and P_j is the jamming power. Indicator function $\phi(i) = 1$, if the adversary is in a jamming state in the i-th block; otherwise $\phi(i) = 0$. Channel gains, $G_m(i)$, $G_e(i)$, and $G_z(i)$ are defined to be the independent complex gains of transmitter-to-receiver channel, transmitter-to-adversary channel, and adversary-to-receiver channel, respectively (as illustrated in Figure 1). Associated power gains are denoted with $H_m(i) = |G_m(i)|^2$, $H_e(i) = |G_e(i)|^2$, and $H_z(i) = |G_z(i)|^2$. We assume that channel reciprocity principle is valid for all channels, i.e., reverse channels and forward channels have identical gains. We also assume that joint probability density function of instantaneous power gains, $f_{\mathbf{H}}(\mathbf{h})$, where $\mathbf{H} = [H_m(\cdot)\ H_e(\cdot)\ H_z(\cdot)]$, is well defined and known by all entities.

B. Methods for Obtaining CSI and Adversary Model

The legitimate transmitter may choose to obtain main CSI or communicate without it. We call the latter strategy the *no CSI case*. In either case, the transmitter sends training symbols to the legitimate receiver at the beginning of each time block. In this paper, we ignore the overhead associated with this training process. We assume that, using the training symbols sent at the beginning of block i, the legitimate receiver obtains perfect knowledge of $g_m(i)$[1] and the adversary obtains perfect knowledge of $g_e(i)$.

Once the receiver observes main CSI, it uses two possible methods for feeding back this information. The first one is directly feeding back the observed channel state: the value of $g_m(i)$ is encoded at the receiver and sent to the transmitter in a feedback packet. Thus, we call this feedback method the *packet feedback*. We assume that the legitimate receiver and the adversary both decode this packet successfully and learn $g_m(i)$. The second method is using pilot based CSI feedback in which the receiver sends training symbols to the transmitter. We call this second method the *pilot feedback*. We assume that by using these reverse training symbols, the legitimate transmitter obtains perfect knowledge of $g_m(i)$ and the adversary obtains the perfect knowledge of $g_z(i)$. Thus, in the first method, the adversary obtains the knowledge of $g_m(i)$, but not $g_z(i)$, whereas the reverse is true in the second method. We denote the vector of channel power gains observed by the adversary at the beginning of the ith block with $h_A(i)$.

The strategy space of the adversary in each block is binary: jamming ($\phi(i) = 1$) or eavesdropping ($\phi(i) = 0$). The transmitter does not observe the strategy of the adversary in any given block. The strategy of the adversary from one block to the next is arbitrary. Hence, the legitimate pair has to select the communication rate such that the communication has to be secure and reliable under any possible strategy of the adversary.

C. Problem Formulation

The secrecy level of a transmitted message w is measured by the equivocation rate at the adversary. The equivocation rate at the adversary is defined as the entropy of the transmitted message conditioned on the channel output and the available CSI at the adversary.

Our goal is to find secrecy rates, R_s, that is achievable under any strategy of the adversary. A secrecy rate R_s is said to be

[1]The realizations of the random variables are represented by lower case letters in the sequel.

achievable if, for any $\epsilon > 0$, there exists a sequence of length NM channel codes for which the following are satisfied under any strategy of the adversary, $\{\phi(k)\}_{1\leq k\leq M}$:

$$P_e^{NM} \leq \epsilon \tag{3}$$

$$\frac{1}{MN} H\left(W|Z^{MN}, h_A^M\right) \geq R_s - \epsilon \tag{4}$$

for sufficiently large N and M and for any $h_A^M \in \mathcal{A}_M$ such that $P[\mathcal{A}_M] = 1$.

In addition to the previously mentioned feedback schemes, we also employ a plain ARQ scheme in some cases, which requires 1-bit negative acknowledgment (NAK) signal at the end of a block. Transmissions that receive a NAK are retransmitted until they are decoded successfully. If the plain ARQ scheme is used, constraint (4) is replaced with the following constraint

$$\frac{1}{MN} H\left(W_s|Z^{MN}, h_A^M, \{\text{NAK}(i)\}_{1\leq i\leq M}\right) \geq R_s - \epsilon \tag{5}$$

Here, we assume that 1-bit NAK signals are obtained at the transmitter and the adversary error free.

III. Results

In this section, we summarize our results concerning the transmission of a secrecy message over many blocks. We first present a secrecy rate that is achievable under the no CSI case. We also show that this rate is a tight lower bound to the capacity when the channel power gains satisfy a certain condition. Then, we find an upper bound to the secrecy rates that are achieved with the main channel feedback.

Theorem 1. *The achievable secrecy rate under no CSI case is given by*

$$R_s^{\text{No CSI}} = \left[E\left[\log\left(1 + \frac{PH_m}{1+P_jH_z}\right) - \log\left(1+PH_e\right)\right]\right]^+ \tag{6}$$

Note that $R_s^{\text{No CSI}}$ is achievable under any adversary strategy, $\phi(i)_{1\leq i\leq M}$. The proof is based on Wyners original scheme [4]. We consider the effect of the adversary's arbitrary strategy on both the probability error and secrecy analysis. The encoder employs a codebook c that contains $2^{R_m NM}, R_m = E\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right)\right]$, independently and identically generated codewords, x^{NM} of lenghth NM. The decoder artificially generates a noise sequence, when the adversary is in the eavesdropping state. Hence, the decoder can employ typical set decoding [11]. The details of the proof is available in [12]. We have the following remark.

Remark: When the channel power gains satisfy

$$\frac{h_m}{\frac{1}{P} + \frac{Ph_z}{P_j}} \geq h_e, \tag{7}$$

for all realizations, $h_m, h_e,$ and h_z then, the achievable rate in (6) is the capacity of the no CSI case. The converse follows from the following upper bound:

$$R_s^{\text{No CSI}} \leq E\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right) - \log\left(1+PH_e\right)\right]^+ \tag{8}$$

Here, note that positive operator is inside the expectation. The proof sketch is as follows. Suppose that $R_s^{\text{No CSI}}$ is achievable rate in the no CSI case. From the definition (3)-(4) and Fano's inequality, we have

$$\min_{\phi(i):1\leq i\leq M} \frac{1}{NM} H\left(W|Z^{NM}, h_e^M\right) \geq R_s^{\text{No CSI}} - \delta_{NM} \tag{9}$$

$$\max_{\phi(i):1\leq i\leq M} \frac{1}{NM} H\left(W|Y^{NM}, h_m^M, h_z^M\right) \leq \epsilon_{NM} \tag{10}$$

for any $h_e^M \in \mathcal{A}_M$ and for any $(h_m^M, h_z^M) \in \mathcal{B}_M$ with $P(\mathcal{A}_M) = 1$ and $P(\mathcal{B}_M) = 1$, respectively. Here, δ_{NM} and ϵ_{NM} go to zero as $N \to \infty$ and $M \to \infty$. The attacker strategies $\phi(i) = 0$, $1 \leq \forall i \leq M$ and $\phi(i) = 1$, $1 \leq \forall i \leq M$ solve LHS of (9) and (10), respectively. Hence, we have

$$\frac{1}{NM} H\left(W|\hat{Z}^{NM}, h_e^M\right) \geq R_s^{\text{No CSI}} - \delta_{NM} \tag{11}$$

$$\frac{1}{NM} H\left(W|\hat{Y}^{NM}, h_m^M, h_z^M\right) \leq \epsilon_{NM} \tag{12}$$

where

$$\hat{Y}^N(i) = g_m(i)X^N(i) + g_z(i)S_j^N(i) + S_m^N(i), \text{ and} \tag{13}$$

$$\hat{Z}^N(i) = g_e(i)X^N(i) + S_e^N(i), \qquad 1 \leq \forall i \leq M. \tag{14}$$

Upper bound (8) follows when we combine (11) and (12). The complete proof is available in [12]. When the condition (7) is satisfied, the term in the expectation in (6) is positive for all the realizations of the power gains.

The result in Theorem 1 can be extended to a multiple adversaries case in which there are K half duplex adversaries and each adversary has an arbitrary strategy from one block to the next.

Corollary 2. *The achievable secrecy rate for the multiple adversary scenario under the no CSI case is given by*

$$R_s^{\text{No CSI}} = \left[\min_{1\leq i\leq K} E\left[\log\left(1+\frac{PH_m}{1+P_j\hat{H}_z}\right) - \log\left(1+PH_{e_i}\right)\right]\right]^+ \tag{15}$$

where K is the number of the adversaries, $\hat{H}_z = \sum_{i=1} H_{z_i}$, H_{z_i} is the power gain of the channel between the receiver and i-th adversary, and H_{e_i} is the power gain of the channel between the transmitter and i-th adversary.

Note that if all H_{e_i}s are identically distributed, rates in (6) and (15) are identical. The proof of Corollary 2 is similar to the proof of Theorem 1 and can be found in [12].

We next analyze the scenario in which there is a main channel feedback. We find an upper bound to the secrecy rates that are achieved with the following strategy. The transmitter uses a rate adaptation scheme to utilize the main channel feedback. The transmitter chooses h_z^* and generates a codebook of size $N\log\left(1+\frac{Ph_m(i)}{1+P_jh_z^*}\right)$ in each block. When the event $\{H_z(i)\phi(i) > h_z^*\}$ occurs, the decoding error occurs and the receiver sends back 1 bit NAK signal. On the next block, the transmitter sends the same bit sequence. Any secrecy rate

achieved with this scheme can be upper bounded by

$$R_s^+ = E\left[\log\left(1+\frac{PH_m}{1+P_jH_z}\right) - \log(1+PH_e) \;\middle|\; H_z \le h_z^*\right]^+ \times P[H_z \le h_z^*] \quad (16)$$

The proof of the upper bound can be found in [12]. By comparing the upper bound given in (16), we gain understanding on the performance of no CSI case. In particular, whenever the achievable rate with the no CSI case exceeds this bound, we know for sure that no CSI is preferable over the case with CSI. The main difference is that, in the CSI case, the unsuccessfully received packets are discarded, whereas in the no CSI case, all the information received by the receiver is used to decode the message. The set of parameters for which this is the case is illustrated in Section V in an example.

IV. Delay Limited Scenario

In this section, we aim to analyze the delay limited scenario in which the legitimate transmitter encodes a separate secret message, $w_s(i) \in \{1,2,\dots,2^{NR_s}\}$ in each block i, $1 \le i \le M$ and each message $w_s(i)$ has to be decoded at the end of block i. Consequently, we use Wyner codes [4] $\mathcal{C}\left(R(h_m(i)), R_s, N\right)$ for each block, where Gaussian codebook of size $2^{NR(h_m(i))}$ is utilized to convey the message $w_s(i)$.

The goal of the transmitter is to maximize the secrecy rate, R_s that satisfies an outage constraint under any adversary strategy, $\phi(i)$. We first define the outage events. For the rate pairs $(R(h_m(i)), R_s)$, the secrecy and connection outage events [3] occur if

$$\frac{I\left(X^N; Z^N | h_a(i), \phi(i)\right)}{N} > R(h_m(i)) - R_s \quad \text{and} \quad (17)$$

$$\frac{I\left(X^N; Y^N | h_m(i), h_z(i), \phi(i)\right)}{N} < R(h_m(i)), \quad (18)$$

respectively, where Y^N and Z^N are defined in (1) and (2), $X^N \sim \mathcal{CN}(\mathbf{0}, PI_{N\times N})$, and h_a is the available channel power gains at the adversary. For the transmission of M separate messages, the constraint maximization problem is formulated as

$$R_s^* = \max_{(R_s, R(h_m))\in\mathcal{F}} R_s \quad (19)$$

where

$$\mathcal{F} = \left\{(R_s, R(\cdot)) : \min_{\{\phi(i)\}_{1\le i\le M}} \frac{1}{M}\sum_{i=1}^{M} I_C(i) I_S(i) \ge \alpha\right\}. \quad (20)$$

Here, $I_C(i)$ and $I_S(i)$ are indicator functions that take on a value 0 in case of a connection and a secrecy outage. The feasible set, $\mathcal{F}$ of Problem (19) contains rate pairs $(R_s, R(\cdot))$ such that the fraction of packets that are not in both secrecy and connection outages are larger than a threshold under any possible adversary strategy. With the following lemma, we show that as the number of messages to be transmitted goes to infinity, Problem (19) can be written with a well defined constraint.

Lemma 3. *As $M \to \infty$, Problem (19) has the same solution as:*

$$R_s^* = \max_{R(h_m), R_s} R_s \quad (21)$$

subject to

$$P\left[R_s + \log\left(1+PH_e\right) \le R(H_m) \le \log\left(1+\frac{PH_m}{1+P_jH_z}\right)\right] \ge \alpha \quad (22)$$

where $R(h_m) = R$ for any h_m in the no CSI case.

Proof. To find $\min_{\{\phi(i)\}} \frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i)$, we first find a lower bound to $\frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i)$ with the following steps.

$$\frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i) = \frac{1}{M}\sum_{i=1}^{M} \phi(i) I_{R(h_m(i)) \le \log\left(1+\frac{Ph_m(i)}{1+P_jh_z(i)}\right)} + (1-\phi(i)) I_{\log(1+Ph_e(i))+R_s \le R(h_m(i)) \le \log(1+Ph_m(i))} \quad (23)$$

$$\ge \frac{1}{M}\sum_{i=1}^{M} \phi(i) I_{R(h_m(i)) \le \log\left(1+\frac{Ph_m(i)}{1+P_jh_z(i)}\right)} + (1-\phi(i)) I_{\log(1+Ph_e(i))+R_s \le R(h_m(i)) \le \log\left(1+\frac{Ph_m(i)}{1+P_jh_z(i)}\right)} \quad (24)$$

$$= \frac{1}{M}\sum_{i=1}^{M} I_{\log(1+Ph_e(i))+R_s \le R(h_m(i)) \le \log\left(1+\frac{Ph_m(i)}{1+P_jh_z(i)}\right)} \quad (25)$$

where RHS of (23) follows from the computation of LHS of (17) and (18) and for the no CSI case $R(h_m)$ is replaced with R in the above derivations. One can check that if $\phi(i) = I_{\log(1+Ph_e(i))+R_s \le R(h_m(i))}$ ($\phi(i) = I_{\log(1+Ph_e(i))+R_s \le R}$ for the no CSI case), then $\frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i)$ equals to (25). From strong of large number theorem, (25) converges to LHS of (22) for all $\{h_m, h_e, h_z\} \in \mathcal{A}$ with $P(\mathcal{A}) = 1$ □

We now consider the case in which the adversary has a specific strategy such that $\phi(i) = I_{h_a(i)\in A_p}$ where A_p is an arbitrary set. The strategy of the adversary is stationary and it is a function of only the available CSI. We address Problem (19) with the following feasible set:

$$\mathcal{F} = \left\{(R_s, R(\cdot)) : \min_{A_p} \frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i) \ge \alpha\right\} \quad (26)$$

that replaces (20).

Theorem 4. *The solution of Problem (19) with the feasible set (26) leads to the following ordering of the achievable rate with respect to the type of feedback:*

$$R_s^{\text{No CSI}} \le R_s^{\text{Packet feedback}} \le R_s^{\text{Pilot Feedback}} \quad (27)$$

Proof. The basic idea is to compare the feasible sets, $\mathcal{F} = \left\{(R_s, R(\cdot) : \min_{A_p} \frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i) \ge \alpha\right\}$. Define $A_p^* = \arg\min \frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i)$. For the no CSI and packet CSI cases, A_p^* are $\{h_e, h_m : \log\left(1+Ph_e(i)\right) + R_s \le R(h_m(i))\}$ and $\{h_e : \log\left(1+Ph_e(i)\right) + R_s \le R\}$, respectively. Then we have $\mathcal{F}^{\text{No CSI}} \subset \mathcal{F}^{\text{Packet Feedback}}$. We have $\mathcal{F}^{\text{Packet Feedback}} \subset$

$\mathcal{F}^{\text{Pilot Feedback}}$ since $\frac{1}{M}\sum_{i=1}^{M} I_C(i)I_S(i)$ that corresponds to A_p^* equals to (25). □

The above theorem implies that the main CSI, which is obtained with packet feedback is more valuable for the adversary than the jammer CSI, which is obtained with pilot feedback. In Section V, we evaluate R_s^* for three cases.

V. Numerical Evaluation

We first analyze the delay-limited case. We assume that both main and eavesdropper channels are characterized by block Rayleigh fading, where the main channel and eavesdropper channel power gains follow an exponential distribution with a mean 10 and 1, respectively[2]. We also assume the jamming channel does not experience fading, where power gain is equal to 1. The transmission power, P, and the jamming power, P_j are identical and chosen to be 1. In Figure 2(a), we plot the secrecy rate, R_s, as a function of the outage constraint threshold, α under the no CSI, the packet feedback, and the pilot feedback cases. The achievable rates in Figure 2(a) follow the same ordering as given in Theorem 4.

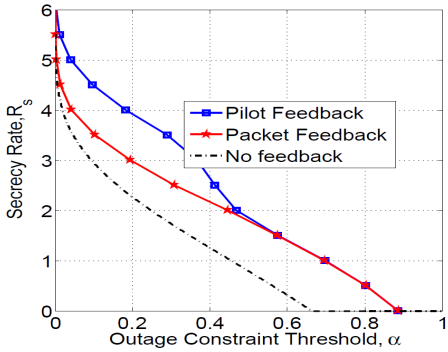
Next, we simulate the ergodic scenario and compare rate (6) achieved at the no CSI case and upper bound (16). We used the same power parameters as in the simulations for the delay-limited case. All three channels are assumed to be block Rayleigh-fading wtih $E[H_z] = 1$ We select the encoding parameter, h_z^* such that $P[H_z \leq h_z^*] = 0.75$.

In Figure 2(b), we illustrate the region where achievable rate (6) is higher than upper bound (16) on the $(E[H_e], E[H_m])$ space. The region to the left of the border, given in the plot contains the set of $(E[H_e], E[H_m])$ for which no CSI case results in a higher secrecy rate. The intuition behind this observation is that, when $E[H_m]$ is much larger than $E[H_e]$, the positive operator inside the upper bound, R^+ loses its significance.

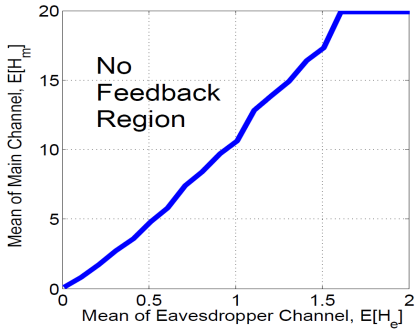
VI. Conclusion

We consider the wiretap channel model under the presence of half duplex adversary that is capable of either jamming or eavesdropping at a given time. We analyzed the achievable rates under a variety of scenarios involving different methods for obtaining transmitter CSI. In particular, we considered no CSI, CSI with packet based feedback, and CSI with pilot based feedback. Each method provides a different grade of information not only to the transmitter on the main channel, but also to the adversary on all channels. We show for the delay limited scenario that, the highest secrecy rate is achieved with the pilot based feedback. In the ergodic case, we showed that in certain cases no CSI may lead to a higher achievable secrecy rates than with CSI.

[2]Such a difference may occur in the cellular setting, when the receiver is a base station with many antennas or in a wireless LAN setting, where the receiver is located at a favorable position for reception, compared to an external adversary.



(a) Delay Limited Scenario



(b) Ergodic Senario

Fig. 2. (a) Comparison of CSI feedback methods under the outage constraint. (b) The region where rate in Theorem 1 outperforms upper bound (16).

References

[1] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. on Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[2] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[3] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels,"*IEEE Trans. Inf. Theory*,vol. 55, no. 4, pp. 1575–1590, Apr. 2009.

[4] A. D.Wyner, "The wire-tap channel". *Bell Syst. Tech. J.*, 54(8):1355–1387, October 1975.

[5] T. L. Marzetta and B. M. Hochwald, "Fast transfer of channel state information in wireless systems," *IEEE Trans. Signal Process.*, vol. 54, no. 4, pp. 1268–1278, Apr. 2006.

[6] G. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast fading channels: A block-Markov Wyner secrecy encoding scheme," *IEEE Trans. on Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, July 2012.

[7] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper,"*IEEE Trans. Signal Process.*, vol. 61, no. 1, Jan. 2013.

[8] X. Zhou, B. Maham, and A. Hjrungnes, "Pilot Contamination for Active Eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

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

[10] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, Compound wiretap channels, *EURASIP J. Wireless Commun. Netw.*, pp. 1-13, 2009, Article 142374.

[11] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York: Wiley, 1991

[12] Y. O. Basciftci, C. E. Koksal and F. Ozguner,"To obtain or not to obtain CSI in the presence of hybrid attacker," http://arxiv.org/abs/1301.6449,