© 2014 IJIRT | Volume 1 Issue 6 | ISSN : 2349-6002

A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel

KARAN LEHKRA, ANIL , VIKAS

DRONACHARYA COLLEGE OF ENGINEERING

Abstract: **Recently, the secrecy capacity of the multi-antenna wiretap channel was characterized by Khisti and Wornell [1] using a Sato-like argument. This note presents an alternative characterization using a channel enhancement argument. This characterization relies on an extremal entropy inequality recently proved in the context of multi-antenna broadcast channels, and is directly built on the physical intuition regarding to the optimal transmission strategy in this communication scenario.**

I INTRODUCTION

Consider a multi-antenna wiretap channel with nt transmit antennas and nr and ne receive antennas at the legitimate receiver and the eavesdropper, respectively:

$$\mathbf{y}_r[m] = \mathbf{H}_r\mathbf{x}[m] + \mathbf{w}_r[m] \qquad (1)$$
$$\mathbf{y}_e[m] = \mathbf{H}_e\mathbf{x}[m] + \mathbf{w}_e[m]$$

where $\mathbf{H}_r \in \mathbb{R}^{nr\times nt}$ and $\mathbf{H}_e \in \mathbb{R}^{ne\times nt}$ are the channel matrices associated with the legitimate receiver and the eavesdropper. The channel matrices $\mathbf{H}_r$ and $\mathbf{H}_e$ are assumed to be fixed during the entire transmission and are known to all three terminals. The additive noise $\mathbf{w}_r[m]$ and $\mathbf{w}_e[m]$ are white Gaussian vectors with zero mean and are independent across the time index m. The channel input satisfies a total power constraint

$$\frac{1}{n}\sum_{m=1}^{n} \|\mathbf{x}[m]\|^2 \le P. \qquad (2)$$

The secrecy capacity is defined as the maximum rate of communication such that the information can be decoded arbitrarily reliably at the legitimate receiver but not at the eavesdropper.

For a discrete memoryless wiretap channel $P(Y_r,Y_e|X)$, a single-letter expression for the secrecy capacity was obtained by Csisz´ar and K¨orner [2] and can be written as

$$C = \max_{P(U,X)} [I(U;Y_r) - I(U;Y_e)] \qquad (3)$$

where U is an auxiliary random variable over a certain alphabet that satisfies the Markov relation U − X − (Yr,Ye). Moreover, (3) extends to continuous alphabet cases with power constraint, so the problem of characterizing the secrecy capacity of the multi-antenna wiretap channel reduces to evaluating (3) for the specific channel model (1) .

Note that evaluating (3) involves solving a functional, nonconvex optimization problem. Solving optimization problems of this type usually requires nontrivial techniques and strong inequalities. Indeed, for the single-antenna case (nt = nr = ne = 1), the capacity expression (3) was successfully evaluated by Leung and Hellman [3] using a result of Wyner [4] on the degraded wiretap channel and the celebrated entropy-power inequality [5, Cha. 16.7]. (Alternatively, it can also be evaluated using a classical result from estimation theory via a relationship between mutual information and minimum mean-squared error estimation [6].) Unfortunately, the same approach does not extend to the multi-antenna case, as the latter, in its general form, belongs to the class of nondegraded wiretap channels. The problem of characterizing the secrecy capacity of the multi-antenna wiretap channel remained open until the recent work of Khisti and Wornell [1].

In [1], Khisti and Wornell followed an indirect approach to evaluate the capacity expression (3) for the multi-antenna wiretap channel. Key to their evaluation is the following genie-aided upper bound

$$
\begin{aligned}
I(U;Y_r) - I(U;Y_e) &\leq I(U;Y_r,Y_e) - I(U;Y_e) && (4)\\
&= I(X;Y_r,Y_e) - I(X;Y_e) - [I(X;Y_r,Y_e|U) - I(X;Y_e|U) && (5)\\
&\leq I(X;Y_r,Y_e) - I(X;Y_e) && (6)\\
&= I(X;Y_r|Y_e) && (7)
\end{aligned}
$$

where (5) follows from the Markov chain $U - X - (Y_r,Y_e)$, and (6) follows from the trivial inequality $I(X;Y_r,Y_e|U) \geq I(X;Y_e|U)$. Khisti and Wornell [1] further noticed that the original objective of optimization $I(U;Y_r) - I(U;Y_e)$ depends on the channel transition probability $P(Y_r,Y_e|X)$ only through the marginals $P(Y_r|X)$ and $P(Y_e|X)$, whereas the upper bound $I(X;Y_r|Y_e)$ does depend on the *joint* conditional $P(Y_r,Y_e|X)$. A good upper bound on the secrecy capacity is thus contrived as

$$C = \max_{P(U,X)} [I(U;Y_r) - I(U;Y_e)] \leq \min_{P(Y_r',Y_e'|X)\in\mathcal{D}} \max_{P(X)} I(X;Y_r'|Y_e') = \max_{P(X)} \min_{P(Y_r',Y_e'|X)\in\mathcal{D}} I(X;Y_r'|Y_e') \quad (8)$$