GMM signaling for secret transmissions over MIMOME Gaussian channels

Francesco Renna

Instituto de Telecomunicações and Universidade do Porto, frarenna@dcc.fc.up.pt

Nicola Laurenti and Stefano Tomasin

University of Padova, {nil, tomasin}@dei.unipd.it

I. Introduction

In this work, we consider the problem of securing communication via physical layer techniques between two legitimate nodes, Alice and Bob, in the presence of a passive eavesdropper, Eve, when all three terminal are assumed to deploy multiple antennas, i.e., in the presence of a multiple-input multiple-output multiple-eavesdropper (MIMOME) channel. In particular, we evaluate strong secrecy rates, i.e., transmission rates for which reliable reception at Bob can be guaranteed, while Eve gains negligible information on the transmitted signal, that are achievable when Alice and Bob are assumed to have perfect channel state information (CSI) of the legitimate channel, whereas they know only the statistics of the eavesdropper channel. On the other hand, we also assume that the legitimate nodes can leverage a physical advantage with respect to the eavesdropper. Namely, on denoting by $n, m_{\rm b}$ and $m_{\rm e}$ the number of antennas at Alice, Bob and Eve, respectively, we assume that $n \geq m_{\rm b} > m_{\rm e}$. This is the case for instance of a base station (with many antennas) transmitting to a relay (with fewer antennas) while being intercepted by a terminal (with even fewer antennas).

Such transmission scenario has also been considered in [1], where achievable secrecy rates are derived by considering wiretap coding techniques and Gaussian codebooks. On the other hand, in this work, we focus on a novel signaling scheme, which generalizes the one described in [2], where signals transmitted over the MIMOME channel are random vectors picked from a Gaussian mixture model (GMM) distributions, and information is carried by the index of the single Gaussian component from which the signal is drawn.

II. Achievable secrecy rates with GMM signaling

We assume that Alice and Bob agree before transmission on a set of K mean vectors, $\boldsymbol{\mu}_k \in \mathbb{R}^n$, $k = 1, \ldots, K$, and K covariance (positive semidefinite) matrices $\boldsymbol{\Sigma}_k \in \mathbb{R}^{n \times n}$, $k = 1, \ldots, K$, and that means and covariances are also known to Eve. Then, at each transmission Alice encodes by an error correcting code the message u into a message $c \in \{1, \ldots, K\}$ with probability mass function (pmf) $\{p_1, p_2, \ldots, p_K\}$ that is sent by generating vector $\boldsymbol{x}$ at random, taken from the multivariate normal distribution $\mathcal{N}(\boldsymbol{\mu}_c, \boldsymbol{\Sigma}_c)$. Note that, in our scenario, the information carried by the transmitted signal is associated with the particular realization of the random variable c, rather than the actual value of the vector $\boldsymbol{x}$.

A. High-SNR secrecy capacity

The following theorems characterize the secrecy rates that are achieved by the proposed signaling strategy in the high-signal-to-noise ratio (SNR) regime.

Theorem 1: Denote by $C_{\rm s}$ the secrecy capacity associated with the MIMOME system described in Section I with GMM transmission and discrete input $c \in \{1, \ldots, K\}$. Then, the high-SNR secrecy capacity is given by

$$C_{\rm s}^{\infty} = \lim_{\rm SNR \to \infty} C_{\rm s} = \log K. \tag{1}$$

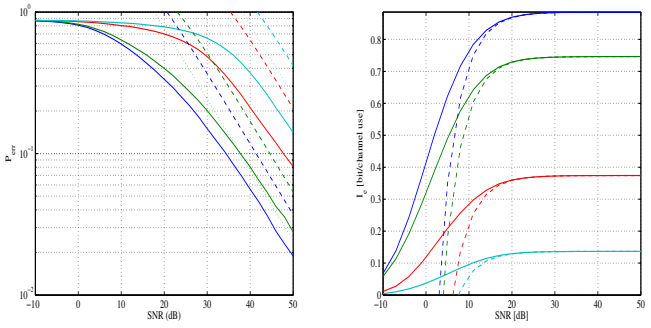
Remarkably, the high-SNR secrecy capacity is asymptotically achieved by properly designing the GMM that describes the input signal $\boldsymbol{x}$ so that the information leakage to the eavesdropper can be driven arbitrarily close to zero. This is obtained by picking the K Gaussian distributions such that the range

space of covariance matrices overlap enough as to be indistinguishable by Eve. At the same time reliable detection at Bob is still possible due to the larger number of antennas $m_{\rm b}$. Thus, zero mutual information leakage at Eve is guaranteed almost surely (i.e., with probability 1 with respect to the eavesdropper channel statistics), and random wiretap coding techniques are not needed to achieve secrecy capacity in the limit $\mathrm{SNR} \to \infty$.

B. Reliability vs. secrecy tradeoff

When the SNR cannot be assumed arbitrarily large, mutual information at the eavesdropper cannot be made to vanish without compromising also reception at Bob. Therefore, in this case, we characterize the tradeoff between reliability and secrecy by providing a description of (an upper bound to) the symbol error probability at Bob and (an upper bound to) the mutual information at Eve.

Theorem 2: Let $\bar{P}_{\rm err}(\mathrm{SNR})$ denote the Bhattacharyya upper bound [3] to the symbol error probability for the legitimate receiver associated with the MIMOME system described in Section I with GMM transmission with $\boldsymbol{\mu}_c = \mathbf{0}$ and discrete input $c \in \{1, \ldots, K\}$. In the high-SNR regime such upper bound can be expanded as



(a) Upper bound and true symbol error probability at Bob.

(b) Upper bound to the mutual information at Eve and its expansion (3).

Fig. 1. Tradeoff between error probability at Bob and mutual information leakage at Eve.

$$\bar{P}_{\rm err} = (g_c \cdot \mathrm{SNR})^{-d} + o\left((\mathrm{SNR})^{-d}\right) \quad , \quad d = \begin{cases} (m_{\rm b} - s_{\max})/2 & , \text{ if } s_{\max} < m_{\rm b} < 2s_{\max} \\ s_{\max}/2 & , \text{ if } m_{\rm b} \geq 2s_{\max} \end{cases} , \qquad (2)$$

where the diversity-order d [4] determines the slope of the upper bound to the error probability curve in a logarithmic plot, and $s_{\max} \in \mathbb{N}$ is a parameter chosen by the transmitter which must satisfy $m_{\rm e} \leq s_{\max} < m_{\rm b}$. On the other hand, the coding gain g_c [4] represents the power offset of the error probability curve and is a function of the channel gains at Bob and the input covariance matrices.

Theorem 3: Let $\bar{I}_{\rm e}(\mathrm{SNR})$ denote an upper bound to the mutual information at the Eve associated with the MIMOME system described in Section I with GMM transmission with $\boldsymbol{\mu}_c = \mathbf{0}$ and discrete input $c \in \{1, \ldots, K\}$ and for a given eavesdropper channel realization $\boldsymbol{\Phi}_{\rm e} \in \mathbb{R}^{m_{\rm e} \times n}$. In the high-SNR regime such upper bound can be expanded as

$$\bar{I}_{\rm e}(\mathrm{SNR}) = \bar{I}_{\rm e}(\infty) + \bar{I}'_{\rm e}(\infty) \cdot (1/\mathrm{SNR}) + o(1/\mathrm{SNR}), \qquad (3)$$

with $\bar{I}_{\rm e}(\infty)$ and $\bar{I}'_{\rm e}(\infty)$ not depending on the SNR (full expressions provided in the paper).

III. Preliminary Numerical Results and Conclusions

Numerical results are reported for a MIMOME scenario with $n = 15, m_{\rm b} = 6, m_{\rm e} = 4$, $K = 8$ and $s_{\max} = 5$. Fig. 1 shows the values of the upper bound on the symbol error probability and the true error probability, with the corresponding values of the upper bound of the mutual information leakage at Eve and its expansion (3), for different SNR values. Different colors in plots represents different sets $\{\boldsymbol{\Sigma}_k\}$ of covariance matrices, with different degrees of overlapping among their ranges. The tradeoff between the information leakage to Eve and the error probabilities at Bob is clearly visible.

References

[1] X. He and A. Yener, "MIMO wiretap channels with arbitrarily varying eavesdropper channel states," *CoRR*, vol. abs/1007.4801, 2010.

[2] G. Reeves, N. Goela, N. Milosavljevic, and M. Gastpar, "A compressed sensing wire-tap channel," *CoRR*, vol. abs/1105.2621, 2011.

[3] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification (2nd Edition)*. New York, NY: Wiley-Interscience, 2000.

[4] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744–765, March 1998.