Abstract—We consider a Gaussian MISO wiretap channel, where a multi-antenna source communicates with a single-antenna destination in the presence of a single-antenna eavesdropper. The communication is assisted by multi-antenna helpers that act as jammers to the eavesdropper. Each helper independently transmits noise which lies in the null space of the channel to the destination, thus creates no interference to the destination. Under the assumption that there is eavesdropper channel uncertainty, we derive the optimal covariance matrix for the source signal so that the secrecy rate is maximized subject to probability of outage and power constraints. Assuming that the eavesdropper channels follow zero-mean Gaussian model with known covariances, we derive the outage probability in a closed form. Simulation results in support of the analysis are provided.

Index Terms—Gaussian MISO wiretap channel, cooperative jamming, artificial noise, outage probability

I. INTRODUCTION

Physical layer secrecy exploits channel conditions to maximize the rate of reliable information delivered to the legitimate destination, with the eavesdropper being kept as ignorant of that information as possible. This line of work was pioneered by Wyner [1], who showed that when an eavesdropper’s channel is a degraded version of the source-destination channel, the source and destination can exchange secure messages perfectly at a non-zero rate, while the eavesdropper can learn almost nothing about the messages from its observations. The need for physical layer security in the context of wireless communications is motivated by challenges associated with classical cryptographic approaches, most notably the exchange and maintenance of private keys.

The secrecy capacity for multiple antenna wiretap channels with perfect channel state information on the eavesdropper is established in [2], [3], [4] under sum power constraints, and in [5] and [6] under power-covariance constraints. For MISO wiretap channels, the optimal input covariance matrix that achieves the secrecy capacity under a sum power constraint was given in a closed form in [7]. As shown in [8], when the channel to the destination encounters more fading than the channel to the eavesdropper, a positive secrecy rate can not be guaranteed. One way to overcome this problem is to use helpers who amplify-and-forward, or decode-and-forward the source signal, or perform cooperative jamming (CJ). In the latter case, helpers do not need to receive nor relay the source message, but rather just transmit noise to degrade the channel to the eavesdropper, therefore increasing the secrecy rate. In [9], a multiple access wiretap channel was considered and it was shown that if the optimal power allocation policy does not allow a certain user to transmit, that particular user could increase the secrecy rate by transmitting artificial noise. In [10], multiple helpers were employed to transmit a weighted jamming signal that enforces nulling at the legitimate destination and maximize the secrecy rate. Following that work, [11] found the optimal weights by avoiding the nulling at the destination, which achieves higher secrecy rate.

In [12], a MISO system with multi-antenna transmitter and single-antenna legitimate receiver and eavesdropper was studied. The transmitter constructs a Gaussian distributed artificial noise that lies in the null space of its channel to the legitimate receiver, and sends a sum of information bearing signal and the artificial noise, which only confuses the eavesdropper but not the legitimate receiver. Since the transmitter does not know the channel to the eavesdropper, the power of the artificial noise is designed to uniformly spread along the null space. In [13], the use of artificial interference for a MIMO wiretap channel is studied. The transmitter sends a sum of signal and artificial noise. When the CSI of the eavesdropper is unknown, the artificial noise is designed to lie in the null space of the right singular vector associated with the largest singular value of its transmitter-receiver channel matrix, and the power of the noise is uniformly spread along the null space. In [14], the artificial noise is studied in a MISO channel overheard by multiple single-antenna eavesdroppers. The source transmits a mixture of message and artificial noise. Without the CSI of the eavesdroppers, the outage based artificial noise design is formulated, with a so-called safe convex approximation is used to find the solution.

In this paper we consider a MISO wiretap channel with multiple multi-antenna helpers implementing cooperative jamming. A multi-antenna source transmits the message, while each helper transmits jamming noise that lies in the subspace that is orthogonal to the helper-destination channel. Each helper generates jamming noise locally based on only its own link to the receiver. Without any other information, the power of the jamming noise is uniformly spread along the null space. We study the problem of determining the input covariance matrix so that the secrecy rate is maximized subject to a sum power constraint and also an outage probability constraint. The source can determine the optimal input covariance matrix solely based on statistical information about the source-eavesdropper channel, with the channel following a zero mean Gaussian model with identity covariance. Assuming that the helper-eavesdropper channels follow zero-mean Gaussian distributions with arbitrary covariance matrices, the outage probability is as obtained in a closed form. Introducing the outage constraint not only provides quality control but also allows taking the uncertainty of the eavesdropper’s channel into consideration and simplifies the optimization problem with respect to the covariance matrix of the input.

Notation - Throughout this paper, following notations are adopted. Upper case and lower case bold symbols denote matrices and vectors, respectively. Superscripts *, † and ⪰ denote respectively conjugate, transposition and conjugate transposition. Tr(A) denotes the trace of the matrix A. A ⊵ n denotes that the matrix A is Hermitian positive semi-definite. |a| denotes absolute value of the complex number a. ∥a∥ = √a∗a denotes Euclidean norm of the vector a. Iₙ denotes the identity matrix of order n (the subscript is dropped when the dimension is obvious). Cₙᵣ denotes the set of all n × r complex vectors. E{·} denotes the expectation operator. i = √−1. x ~ y denotes x and y have identical distributions.
The power constraint is hence be jamming noise so that it delivers a null at Bob. It is clear that each helper should be equipped with such that there are enough degrees of freedom to design at Bob and Eve with input covariance matrix

antennas (messages to the legitimate receiver, Bob, through the channel shown in Fig. 1. The transmitter Alice uses generated by the helpers; and

signal, jamming noise and additive white Gaussian noise (AWGN).

In order for the noise vector of helper to cause nulling at Bob, let us assume that the nodes do not have any channel information with the following exceptions:

- Alice knows
- Alice has statistical information on
- Helper knows its own link to Bob.

The outage probability is defined as

Let us assume that the nodes do not have any channel information with the following exceptions:

1. Alice knows
2. Alice has statistical information on
3. Helper knows its own link to Bob.

The outage probability is defined as

\[ P_{out}(R) = \min_{Q \succeq 0, \text{Tr}(Q) \leq 1} \text{Pr}(C_1 < R). \]  

We will determine the maximum \( R \) such that the outage probability is below a prescribed small level, \( \epsilon \), which represents the quality of service (QoS). Mathematically, the problem is formulated as

\[ \max_0 R \]  
s.t. \( P_{out}(R) \leq \epsilon. \)

The problem of (10) is equivalent to the problem of maximizing the secrecy rate subject to QoS and power constraints as follows

\[ \max_0 R \]  
s.t. \( Q \succeq 0, \text{Tr}(Q) \leq 1, \text{Pr}(C_1 < R) \leq \epsilon. \)

A. Optimal Input Covariance Matrix Structure

Lemma 1: For the problem of (17), and for \( g_0 \sim \mathcal{CN}(0, \sigma^2 I) \), the optimal \( Q \) is given by \( Q^* = |h_0^* h_0^*| \), and the optimization problem can be written as

\[ \max_0 R \]  
s.t. \( \text{Pr} \left( \frac{\rho_0 |g_0|^2}{\sum_{k=1}^{N} \rho_k (N_k - 1) - 1 ||E_k^* g_k||^2 + 1} > 1 + \rho_0 ||h_0||^2 - 1 \right) \leq \epsilon. \)
The proof is given in Appendix A.

Next, we solve the problem of (13). Obviously, for the optimal $R$, the constraint of (14) holds with equality. Let us define the critical value $\chi_*$ so that
\[
\Pr\left(\frac{\rho_0|g_0|^2}{\sum_{k=1}^N \rho_k(N_k - 1)^{-1}\|E_k g_k\|^2 + 1} > \chi_*\right) = \epsilon.
\] (15)
Then, the optimal $R$ is given by
\[
R^* = \log(1 + \rho_0\|h_0\|^2) - \log(1 + \chi_*).
\] (16)
The condition for $R^* > 0$ is given in the following lemma.

**Lemma 2:** For a given $\epsilon$, $R^* > 0$ if and only if
\[
\Pr\left(\frac{\rho_0|g_0|^2}{\sum_{k=1}^N \rho_k(N_k - 1)^{-1}\|E_k g_k\|^2 + 1} > \chi_0\right) < \epsilon.
\] (17)
To find the critical value $\chi_*$, defined in (15), we can use the bisection method. The calculation of the outage probability is discussed in the following subsection.

**B. Closed Form Outage Probability**

Let us assume that $g_0 \sim CN(0, \sigma^2 I)$ and $g_k \sim CN(0, \Sigma_k)$. In this case, the probability of outage can be found in a closed form as follows.

The calculation of the outage probability involves calculating
\[
\Pr\left(\frac{\rho_0|g_0|^2}{\sum_{k=1}^N \rho_k(N_k - 1)^{-1}\|E_k g_k\|^2 + 1} > \chi_0\right)
\] (18)
which can be rewritten as
\[
\Pr\left(\sum_{k=1}^N \rho_k(N_k - 1)^{-1}\|E_k g_k\|^2 - \frac{\rho_0}{\chi_0}|g_0|^2 < 1\right).
\] (19)
We use the methods in [16] to calculate (19). Note that $E_k g_k \sim CN(0, E_k^\dagger \Sigma_k E_k)$. Let $E_k^\dagger \Sigma_k E_k$ have eigen-decomposition $U_k^\dagger D_k U_k$. Denote
\[
D = \text{diag}\left(\frac{\rho_1}{N_1 - 1} D_1, \ldots, \frac{\rho_N}{N_N - 1} D_N, -\sigma^2 I, -\rho_0/\chi_0\right).
\] (20)
After a few derivations, (19) is equivalent to
\[
\Pr(z^\dagger D z < -1)
\] (21)
where $z \sim CN(0, I_{N+1})$. Let $Y = z^\dagger D z$. $Y$ is an indefinite quadratic form. The results in [16] give the expression for $\Pr(Y \geq y)$. Denote $\xi_0 = \sigma^2 \rho_0/\chi_0$. Let $\nu_1, \ldots, \nu_K$ denote different positive diagonal entries of $D$, with multiplicity $m_1, \ldots, m_K$ and $m_1 + \cdots + m_K = N$. According to the result in [16] Eq. (32) for the case $z \sim CN(0, I_{N+1})$, we have
\[
\Pr(Y \geq y) = -\sum_{k=1}^K \frac{\exp(-y/\nu_k)}{(-\nu_k)^{m_k-1}(m_k - 1)!} \hat{g}_k^{(m_k-1)}(0, y)
\] (22)
where
\[
\hat{g}_k(s, y) = e^{-sy} \frac{1}{(1 + \xi_0/\nu_k + \xi_0 s)^{\nu_k}} \prod_{j=1}^K \frac{1}{(\alpha_{kj} - \nu_j s)^{\nu_j}}.
\] (23)
\[
\alpha_{kj} = \begin{cases} 1 - \nu_j/\nu_k & j \neq k \\ -1 & j = k \end{cases},
\] (24)
\[
\beta_{kj} = \begin{cases} m_j & j \neq k \\ 1 & j = k \end{cases}.
\] (25)

IV. SIMULATION AND ANALYSIS

In simulation, Alice has three antennas, each helper has two antennas. Alice-Eve link $g_0 \sim CN(0, I)$, and $k_{th}$ helper-Eve link $g_k = CN(0, \Sigma_k)$. Alice has SNR $\rho_0 = 5$ dB, and all $N$ helpers have SNR $\rho_k = 2$ dB. Outage probability constraint, $\epsilon = 0.01$, and $P_{out}(R^*) = \epsilon$, where $R^*$ is given in (16). Results are averaged over $10^5$ independent trials. For each trial, generate independent and identical distributed $h_0, h_k = CN(0, I)$. During one trial, $h_0$ is kept as constants. For a $R^* > 0$, lemma 2 has to be satisfied. When $h_0$ is much more degraded than $g_0$, with small number of helpers, the secrecy rate can not be guaranteed to be positive. During each trial, for $N = 5, \cdots, 10$ number of helpers, use bi-section method to search for a larger $R$, satisfying the outage constraint, until it converges to $R^*$. In Fig. 2, the secrecy rate increases when the number of helpers increases. In Fig. 3, since $\Pr(R)$ is a function of $R$, fix $R_1 = 0.6 \log_2(1 + P_1\|h_0\|^2)$, plot the $\Pr(R_1)$, the outage probability decreases when the number of helpers increases. Because Bob is not affected by the noise transmitted by the helpers, but Eve is, and the more helpers, the more confounded Eve will be.

![Fig. 2. Secrecy Rate vs Number of Helpers. $\rho_0 = 5$ dB, $\rho_k = 2$ dB.](image-url)

V. CONCLUSIONS

We proposed a cooperative jamming scheme, where multiple helpers transmit nulling noise to maximize secrecy rate subject to an outage probability constraint, and a power constraint. Assuming that the transmitter only knows its channel to legitimate receiver and the statistical CSI of its channel to eavesdropper, each helper known its own link to receiver, we formulated and solved an outage constrained secrecy rate maximization problem. Simulations show that proposed design could guarantee a low outage probability.
where we have used the fact that if a matrix. First, we notice that this, we write To determine the structure of the optimal constraint Pr(C₁ < R) ≤ ǫ. Thus, it should hold that λ₂ = · · · = λ_N₁ = 0. As a result, we have

Pr(C₁ < R) = Pr(\[
\frac{\rho_0 |g_0|^2}{\sum_{k=1}^{N} \rho_k (N_k - 1) - 1 |E_k^* h_k|^2 + 1} > \rho_0 \frac{|h_0|^2}{2^R} - 1 \frac{2^R}{\lambda_1}.
\] \tag{34})

From (33), we know that \(\frac{\rho_0 |g_0|^2}{2^R} \frac{1}{\lambda_1}\) is increasing with λ₁ but decreasing with R, in other words, a larger λ₁ will allow a larger R without violating the outage constraint Pr(C₁ < R) ≤ ǫ. Since Tr(Q) = λ₁ ≤ 1, it holds that λ₁ = 1. As a result, we have

Pr(C₁ < R) = Pr(\[
\frac{\rho_0 |g_0|^2}{\sum_{k=1}^{N} \rho_k (N_k - 1) - 1 |E_k^* h_k|^2 + 1} > 1 + \rho_0 \frac{|h_0|^2}{2^R} - 1 \frac{2^R}{\lambda_1}.
\] \tag{35})

Based on the result above, the problem of (11) is equivalent to the problem of (13). This completes the proof.

REFERENCES

[1] A. D. Wyner, “The wiretap channel,” Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[2] A. Khisti and G. Wornell, “Secure transmission with multiple antennas: I. The MISO wiretap channel,” IEEE Trans. Inform. Theory, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[3] A. Khisti and G. Wornell, “Secure transmission with multiple antennas: II. The MIMOME wiretap channel,” IEEE Trans. Inform. Theory, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[4] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE Trans. Inform. Theory, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[5] T. Liu and S. Shamai (Shitz), “A note on the secrecy capacity of the multi-antenna wire-tap channel,” IEEE Trans. Inform. Theory, vol. 55, pp. 2547-2553, Jun. 2009.

[6] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), “An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel, ” in Proceedings of the IEEE International Symposium on Information Theory (ISIT), Seoul, Korea, June-July 2009.

[7] J. Li and A. P. Petropulu, “Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels,” in Proc. IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), pp. 3362-3365, 2010.

[8] D. N. C. Tse and P. Viswanath, Fundamentals of Wireless Communications, Cambridge University Press, Cambridge, UK, 2005.

[9] E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming,” IEEE Trans. Inform. Theory, vol. 54, pp. 2735-2751, 2008.

[10] D. Lu, H. Zhu, A. P. Petropulu, and H. V. Poor, “Cooperative jamming for wireless physical layer security,” in Proc. IEEE/SP Workshop on Statistical Signal Processing, pp. 417-420, 2009.

[11] J. Li, S. Weber, and A. P. Petropulu, “Secrecy rate optimization under cooperation with perfect channel state information,” in Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, pp.824-828, Nov. 2009.

[12] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” Proc. IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[13] A. L. Swindlehurst, “Fixed secrecy solutions for the MIMO wiretap channel,” in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2437-2440, 2009.

[14] Q. Li, W. Ma, and A. So, “Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial Noise,” presented at the Asilomar, 2011.

[15] L. Zheng and D. N. C. Tse, “Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels,” IEEE Trans. Inform. Theory, vol. 49, no. 5, pp. 1073-1096, May 2003.

[16] D. Raphaeli, “Distribution of noncentral indefinite quadratic forms in complex normal variables,” IEEE Trans. Inform. Theory, vol. 42, pp. 1002-1007, 1996.