Title

A NEW LOOK AT SECRECY CAPACITY OF MIMOME USING ARTIFICIAL NOISE FROM ALICE AND BOB WITHOUT KNOWLEDGE OF EVE'S CSI

Authors
Sohrabi, Reza
Hua, Yingbo

Publication Date
2018

DOI
10.1109/globalsip.2018.8646640

Peer reviewed

A NEW LOOK AT SECRECY CAPACITY OF MIMOME USING ARTIFICIAL NOISE FROM ALICE AND BOB WITHOUT KNOWLEDGE OF EVE'S CSI

Reza Sohrabi, *Student Member, IEEE,* Yingbo Hua, *Fellow, IEEE*

***Abstract*—This study investigates a secure wireless communication scheme which combines two of the most effective strategies to combat (passive) eavesdropping, namely mixing information with artificial noise at the transmitter and jamming from a full-duplex receiver. All nodes are assumed to possess multiple antennas, which is known as a MIMOME network. The channel state information (CSI) of Eve is known to Eve but not to Alice and Bob. While such setup has been investigated in related works, new and important insights are revealed in this work. We investigate the design of optimal jamming parameters to achieve higher secrecy, and in particular we focus on two important cases corresponding to Bob using either a simple jamming or a smart jamming. Furthermore, simulations are presented to highlight the effectiveness of the proposed strategies.**

***Index Terms*—Secrecy capacity, physical layer security, full-duplex, MIMOME, jamming, artificial noise**

I. Introduction

Physical layer security is increasingly important for wireless networks as the computational power available for breaking encryption at higher layers rapidly advances. Since the work of Wyner [1], the secrecy capacity (or simply secrecy) of wireless channel has been investigated from many different aspects such as in [2]–[19]. These aspects include the analysis of the secrecy of fading channels [2], the secrecy of multi-antenna setups [3]–[5], the secrecy of cooperative jamming with relays or helpers [6], [7], the investigation of secure degrees of freedom [8] and so on. One prominent strategy to enhance wireless secrecy was proposed in [9] in which the authors propose the use of artificial noise from the transmitter (Alice) in the null space of the legitimate channel along with the information signal. Another effective strategy is to equip the receiver (Bob) with the full-duplex radio capability so that it can transmit jamming noise against Eve while Bob (and Eve) is trying to receive the information from Alice [10]–[13].

In this study, we investigate an integration of the above two jamming strategies to achieve higher levels of secrecy. This integration was also investigated in [14] in which the authors propose a joint optimization algorithm to derive the best transmission parameters. They assume two separate sets of antennas for transmission and reception for full-duplex. But they did not take into full consideration the effect of residual self-interference at Bob. There are also other works concerned with similar setups in [15]–[19].

In this paper, we do not assume that Alice and Bob know the CSI of Eve which is in contrast to [15]–[17]. The small-scale-fading CSI of Eve is assumed to be Rayleigh distributed like the prior works. But the large-scale-fading CSI of Eve is based on the most harmful location of Eve subject to a radius constraint, which is in contrast to the assumption of Poisson distribution of Eves [14]. More importantly, we treat separately the cases where Eve may perform the optimal matched filtering (OMF) or a basic matched filtering (BMF) depending on whether Bob uses a smart jamming. The above aspects are examples of what make this work new and significant in light of the prior works.

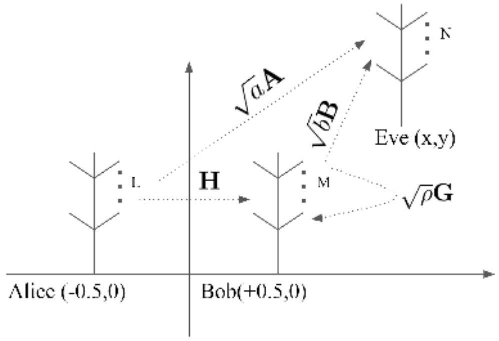

Figure 1: A MIMOME network with full-duplex receiver (Bob)

II. System Model

Our network setup of multiple-input multiple-output multiple-antenna eavesdropping (MIMOME) is shown in Fig. 1, where Alice (of L antennas) intends to send secret information over the wireless channel to Bob (of M antennas) in the presence of possibly many passive Eves (of N antennas each) that may collude with each other at the network layer but not at the physical layer. (Physical layer colluding among distributed Eves is highly difficult in practice.) System parameters are normalized [11] such that the large-scale-fading factor from Alice to Eve is $a = d_A^{-\alpha} = (\sqrt{(x+0.5)^2 + y^2})^{-\alpha}$, and that from Bob to Eve is $b = d_B^{-\alpha} = (\sqrt{(x-0.5)^2 + y^2})^{-\alpha}$. Here, α is the path-loss exponent. It is practical to assume that no Eve is closer to Alice than a certain distance i.e., $d_A \geq \Delta$. The normalized large-scale-fading factor of Bob's self-interference is denoted by ρ. The small-scale-fading channel matrix from Alice to Eve is denoted by $\mathbf{A}$, that from Bob to Eve is $\mathbf{B}$, and that of the self-interference at Bob is $\mathbf{G}$. The channel matrix from Alice to Bob is denoted by $\mathbf{H}$, and its SVD is denoted by

$$\mathbf{H} = \mathbf{U}\sqrt{\mathbf{\Lambda}}\mathbf{V}^H, \tag{1}$$

The authors are with Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521, USA. Emails: rsohr001@ucr.ed, yhua@ece.ucr.edu. This work was supported in part by the Army Research Office under Grant Number W911NF-17-1-0581. The views and conclusions contained in this document are those of the authors only.

978-1-7281-1295-4/18/$31.00 ©2018 IEEE

where $\mathbf{U}$ and $\mathbf{V}$ are unitary matrices, and $\sqrt{\mathbf{\Lambda}}$ is the diagonal matrix that contains the singular values $\sqrt{\lambda_i}$, $i = 1, \cdots, \min(M, L)$, of $\mathbf{H}$ in descending order on its main diagonal. All the elements of all channel matrices are i.i.d. circular complex Gaussian with zero mean and unit variance.

Alice sends the following signal containing secret information and noise:

$$\mathbf{x}_A = \sqrt{\phi P_A}\mathbf{v}_1 s + \sqrt{\frac{(1-\phi)P_A}{L-1}}\mathbf{V}_1\mathbf{w}_A, \tag{2}$$

where $\mathbf{v}_1$ and $\mathbf{V}_1$ are defined by $\mathbf{V} = [\mathbf{v}_1, \mathbf{V}_1]$, s is Alice's information symbol with unit variance (for convenience of exposure of key idea, a single stream of data is studied), and $\mathbf{w}_A$ is an $(L-1) \times 1$ i.i.d. complex Gaussian noise vector with zero mean and unit variance. Also, ϕ is the ratio of Alice's power P_A allocated to information. While Bob receives information from Alice, it also sends a jamming noise. Although a smart jamming will be mentioned later, a simple form of this noise is

$$\mathbf{x}_B = \sqrt{\frac{P_B}{M}}\mathbf{w}_B, \tag{3}$$

where $\mathbf{w}_B$ is an $M \times 1$ i.i.d. complex Gaussian noise vector with zero mean and unit variance. P_A and P_B are powers that are normalized with respect to the path loss from Alice to Bob. The background noises at all nodes are normalized to have the unit variance. Then Bob and Eve receive the following signals, respectively

$$\mathbf{y}_B = \sqrt{\phi\lambda_1 P_A}\mathbf{u}_1 s + \sqrt{\frac{(1-\phi)P_A}{L-1}}\mathbf{U}_1\sqrt{\mathbf{\Lambda}_1}\mathbf{w}_A + \tilde{\mathbf{n}}_B \tag{4}$$

$$\begin{aligned}\mathbf{y}_E =& \sqrt{a\phi P_A}\mathbf{a}_1 s + \sqrt{\frac{a(1-\phi)P_A}{L-1}}\mathbf{A}_1\mathbf{w}_A \\ &+ \sqrt{\frac{bP_B}{M}}\mathbf{B}\mathbf{w}_B + \mathbf{n}_E,\end{aligned} \tag{5}$$

where $\mathbf{AV} = [\mathbf{A}\mathbf{v}_1, \mathbf{A}\mathbf{V}_1] = [\mathbf{a}_1, \mathbf{A}_1]$, $\mathbf{U} = [\mathbf{u}_1, \mathbf{U}_1]$, $\tilde{\mathbf{n}}_B = \sqrt{\frac{\rho P_B}{M}}\mathbf{G}\mathbf{w}_B + \mathbf{n}_B$ which could be modeled as $\mathcal{CN}(\mathbf{0}, (\rho P_B + 1)\mathbf{I})$ [18], $\sqrt{\mathbf{\Lambda}_1}$ is an $(M-1) \times (L-1)$ matrix with $\sqrt{\lambda_i}, i \in \{2, \ldots, \min(M, L)\}$ on the main diagonal. Furthermore, $\mathbf{n}_E$ is an $N \times 1$ i.i.d. complex Gaussian noise vector with zero mean and unit variance.

Since Bob knows the covariance matrix of the noise plus interference in its received signal $\mathbf{y}_B$ in (4), Bob can perform OMF. But due to the orthogonality between $\mathbf{u}_1$ and $\mathbf{U}_1$, the OMF at Bob is equivalent to the BMF at Bob, i.e., $\mathbf{u}_1^H\mathbf{y}_B$ is the sufficient statistic of s given $\mathbf{y}_B$. Since $\mathbf{u}_1^H\mathbf{y}_B = \sqrt{\phi\lambda_1 P_A}s + \mathbf{u}_1^H\tilde{\mathbf{n}}_B$, the optimized SNR for Bob is

$$SNR_{AB} = \frac{\phi\lambda_1 P_A}{1+\rho P_B}. \tag{6}$$

III. Eve using OMF

If Bob uses the simple jamming noise as shown in (3), Eve may have the full knowledge to determine the covariance matrix $\mathbf{R}_E$ of the noise plus interference in its received signal $\mathbf{y}_E$ in (5), i.e.,

$$\mathbf{R}_E = \mathbf{I} + \frac{a(1-\phi)P_A}{L-1}\mathbf{A}_1\mathbf{A}_1^H + \frac{bP_B}{M}\mathbf{B}\mathbf{B}^H. \tag{7}$$

Then Eve can perform the OMF of $\mathbf{y}_E$ by pre-multiplying it by $\mathbf{a}_1^H\mathbf{R}_E^{-1}$, and the optimized SNR at Eve is

$$SNR_{AE} = a\phi P_A\mathbf{a}_1^H\mathbf{R}_E^{-1}\mathbf{a}_1. \tag{8}$$

Then the secrecy capacity [1] of the channel from Alice to Bob against all Eves that may collude at the network layer but not at the physical layer is

$$S = \min_{\text{Eves}}\left(\log(1+SNR_{AB}) - \log(1+SNR_{AE})\right)^+, \tag{9}$$

where $(.)^+ \triangleq \max(0, .)$.

A. Most harmful position of Eve

Although the small-scale-fading CSI of Eve can be reasonably modeled statistically within a period of time of interest (corresponding to a sequence of packets in multiple channel coherent periods in mobile environment), the large-scale-fading CSI of Eve is dependent on the large-scale position of Eve relative to Alice and Bob. For the time of interest in most practical situations (e.g., in the order of seconds or even minutes), the distribution of Eves should typically be considered as unknown and deterministic (but not stochastic and definitely not Poisson distributed). In this case, the best way to handle the unknown large-scale-fading CSI of Eve is to consider the most harmful position of Eve [11]. The notion of average as mentioned later only refers to the average over small-scale-fading. Since SNR_{AB} is invariant to Eve's location, the most harmful Eve is the one whose position maximizes SNR_{AE}. We can write (8) as

$$\begin{aligned}SNR_{AE} =& \phi P_A\mathbf{a}_1^H(\frac{1}{a}\mathbf{I} + \frac{(1-\phi)P_A}{L-1}\mathbf{A}_1\mathbf{A}_1^H \\ &+ \frac{bP_B}{aM}\mathbf{B}\mathbf{B}^H)^{-1}\mathbf{a}_1.\end{aligned} \tag{10}$$

For a fixed $a = d_A^{-\alpha}$, SNR_{AE} is maximized when b is minimum i.e., $b = (1+d_A)^{-\alpha}$. With this b, we have

$$\begin{aligned}SNR_{AE} =& \phi P_A\mathbf{a}_1^H(d_A^\alpha\mathbf{I} + \frac{(1-\phi)P_A}{L-1}\mathbf{A}_1\mathbf{A}_1^H \\ &+ \frac{d_A^\alpha P_B}{(1+d_A)^\alpha M}\mathbf{B}\mathbf{B}^H)^{-1}\mathbf{a}_1.\end{aligned} \tag{11}$$

Conditioned upon $d_A \geq \Delta$, SNR_{AE} is maximized if $d_A = \Delta$. Therefore, the most harmful position of Eve is at $x^* = -0.5 - \Delta$, $y^* = 0$. From now on, we will drop $\min_{\text{Eves}}$ in (9) and refer to a and b as corresponding to the position (x^*, y^*). In all simulations, we will use $\Delta = 0.1$.

B. Optimization

It is easy to prove that S is an increasing function of P_A, but the dependency of S on ϕ and P_B is not trivial. To determine the optimal ϕ and P_B, we are interested to maximize the following objective function:

$$S_L(\phi, P_B) = (\log(1+SNR_{AB}) - \mathbb{E}_{\mathbf{A},\mathbf{B}}[\log(1+SNR_{AE})])^+ \tag{12}$$

[1] Assuming a Gaussian input alphabet, achievable secrecy rate is a better term to be used here [18].

where $\mathbb{E}_x[.]$ denotes expectation with respect to x, and $S_L(\phi, P_B) \leq \mathbb{E}_{\mathbf{A},\mathbf{B}}[S]$ which follows from the fact $(\mathbb{E}[x])^+ \leq \mathbb{E}[(x)^+]$.

We will perform a stochastic maximization of $S_L(\phi, P_B)$, for which we adopt the method proposed in [20]. Our approach is as the following. First, define

$$\begin{aligned} -S_L(\phi, P_B|\mathbf{A},\mathbf{B}) &= -\log(1+\rho P_B + \phi\lambda_1 P_A) \\ &\quad -\log|\mathbf{R}_E| + \log(1+\rho P_B) + \log|\mathbf{R}_E + a\phi P_A \mathbf{a}_1\mathbf{a}_1^H| \\ &= f_1(\mathbf{x}) + f_2(\mathbf{x},\mathbf{A},\mathbf{B}) + f_3(\mathbf{x}) + f_4(\mathbf{x},\mathbf{A},\mathbf{B}), \end{aligned} \tag{13}$$

where f_1, f_2, f_3, and f_4 are defined in the obvious way. With respect to the jamming parameters $\mathbf{x} = [\phi, P_B]^T$, the first two terms are convex and the last two are concave functions. The last two terms can be approximated and upper bounded by their first-order Taylor series expansion iteratively. At iteration t, a random realization of $\mathbf{A}$ and $\mathbf{B}$ is obtained, then given $\mathbf{x}^t = [\phi^t, P_B^t]^T$, and $\mathbf{A}^t$, $\mathbf{B}^t$, let

$$\hat{\mathbf{x}}^t \triangleq \underset{\mathbf{x}\,\in\mathcal{X}}{\arg\min}\, \hat{f}^t(\mathbf{x}), \tag{14}$$

where $\mathcal{X} \triangleq \{\mathbf{x}|0 \leq \phi \leq 1,\ 0 \leq P_B \leq P_B^{max}\}$ and with $\beta^t \in (0,1]$ being a sequence to be properly chosen,

$$\begin{aligned} \hat{f}^t(\mathbf{x}) \triangleq \beta^t \left(f_1(\mathbf{x}) + f_2(\mathbf{x},\mathbf{A}^t,\mathbf{B}^t)\right) + \beta^t(\mathbf{x}-\mathbf{x}^t)^T\mathbf{\Pi}^t \\ + (1-\beta^t)(\mathbf{x}-\mathbf{x}^t)^T(\mathbf{f}^{t-1}) + \tau\|\mathbf{x}-\mathbf{x}^t\|^2 \end{aligned} \tag{15}$$

in which

$$\mathbf{\Pi}^t = \nabla_x \left(f_3(\mathbf{x}) + f_4(\mathbf{x},\mathbf{A}^t,\mathbf{B}^t)\right)|_{\mathbf{x}=\mathbf{x}^t}, \tag{16}$$

and $\mathbf{f}^t$ is a vector that is iteratively updated as

$$\mathbf{f}^t = (1-\beta^t)\mathbf{f}^{t-1} + \beta^t(\mathbf{\Pi}^t + \nabla_x\left(f_1(\mathbf{x}) + f_2(\mathbf{x},\mathbf{A}^t,\mathbf{B}^t)\right)|_{\mathbf{x}=\mathbf{x}^t}). \tag{17}$$

The first term in (15) is the convex part of (13), while the second term is the effect of linearizing the non-convex part. The third term is included to estimate the unknown gradient of $S_L(\phi, P_B)$ (provided $S_L(\phi, P_B) > 0$) by its samples collected over the iterations, which becomes more accurate with each iteration. The last term in (15) is a regularization term. Finally given $\hat{\mathbf{x}}^t$, $\mathbf{x}^t$ is updated as follows with $\gamma^t \in (0,1]$ being a sequence to be properly chosen,

$$\mathbf{x}^{t+1} = (1-\gamma^{t+1})\mathbf{x}^t + \gamma^{t+1}\hat{\mathbf{x}}^t \tag{18}$$

It is worth mentioning that the objective function in (14) is strongly convex and can be optimized easily. Based on conditions stated in [20] for the parameters, the following parameters guarantee convergence in our problem: $\beta^0 = \beta^1 = \gamma^1 = 1$, $\beta^t = \frac{2}{(t+2)^{0.6}}\ \forall\, t \geq 2$, $\gamma^t = \frac{2}{(t+2)^{0.61}}\ \forall\, t \geq 2$, $\tau = 10^{-4}$. The optimization steps are summarized in Algorithm 1. For more details about the theory behind this stochastic optimization and its convergence, please refer to [20]. In Fig. 2, a comparison of $\mathbb{E}_{\mathbf{A},\mathbf{B}}[S]$ based on optimal and non-optimal jamming parameters is presented. The figure shows that in this particular case, the benefit from using full-duplex jamming only ($\phi = 1$, $P_B = P_B^*$) is significantly greater than that from using artificial noise from Alice only ($\phi = \phi^*$, $P_B = 0$), and the combination of the two results in much more improvement of secrecy.

Algorithm 1: Algorithm to perform stochastic optimization

```
Initialize $\phi^0$, $P_B^0$, assign $\phi^{-1} = 0$, $P_B^{-1} = 0$, and choose proper $\beta^t$, $\gamma^t$, $\tau$, $\epsilon$. set $t = 0$.
while $\frac{|\phi^t - \phi^{t-1}|}{\phi^t} + \frac{|P_B^t - P_B^{t-1}|}{P_B^t} > \epsilon$ do
    Make a random realization of $\mathbf{A}, \mathbf{B}$.
    Compute $\hat{\mathbf{x}}^t$ from (14) .
    Update $\mathbf{x}^{t+1}$ using (18).
    Update $\mathbf{f}^t$ using (17).
    $t = t + 1$.
end
Return $\phi^* = \phi^t, P_B^* = P_B^t$.
```

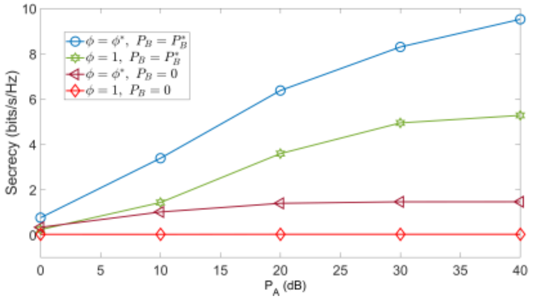

Figure 2: Effect of the optimal jamming parameters on $\mathbb{E}_{\mathbf{A},\mathbf{B}}[S]$ when Eve uses OMF and each node has 4 antennas. 10,000 realizations of $\mathbf{A}$ and $\mathbf{B}$ are used for the simulations.

IV. Eve using BMF

If Bob applies a smart jamming as follows (instead of that in (3))

$$\mathbf{x}_B = \sqrt{\frac{P_B}{n}}\mathbf{Y}\tilde{\mathbf{w}}_B, \tag{19}$$

where $\tilde{\mathbf{w}}_B$ is an $n \times 1$ vector of i.i.d. complex Gaussian noise with unit variance, and $\mathbf{Y}$ is a random $M \times n$ matrix with $M > n$ and the property that $\mathbf{Y}^H\mathbf{Y} = \mathbf{I}$, then Eve is unable to obtain the covariance matrix of the noise plus interference in its received signal. In this case, Eve cannot apply the OMF but the BMF as follows:

$$\begin{aligned} \mathbf{a}_1^H\mathbf{y}_E = \sqrt{a\phi P_A}\|\mathbf{a}_1\|^2 s + \sqrt{\frac{a(1-\phi)P_A}{L-1}}\mathbf{a}_1^H\mathbf{A}_1\mathbf{w}_A \\ + \sqrt{\frac{bP_B}{n}}\mathbf{a}_1^H\mathbf{B}\mathbf{Y}\tilde{\mathbf{w}}_B + \mathbf{a}_1^H\mathbf{n}_E, \end{aligned} \tag{20}$$

and the SNR of this statistics is

$$SNR_{AE} = \frac{\phi a P_A\|\mathbf{a}_1\|^2}{1 + \frac{(1-\phi)}{L-1}aP_A\|\mathbf{A}_1^H\tilde{\mathbf{a}}_1\|^2 + \frac{bP_B}{n}\|\hat{\mathbf{B}}^H\tilde{\mathbf{a}}_1\|^2}, \tag{21}$$

where $\tilde{\mathbf{a}}_1 = \frac{\mathbf{a}_1}{\|\mathbf{a}_1\|}$, and $\hat{\mathbf{B}} = \mathbf{B}\mathbf{Y}$. If $v_1 \triangleq \|\mathbf{a}_1\|^2$, it can be proven that $2v_1$ is distributed as $\chi^2(2N)$. Also if $v_2 \triangleq \|\mathbf{A}_1^H\tilde{\mathbf{a}}_1\|^2$, $2v_2$ is distributed according to $\chi^2(2(L-1))$. Finally, $v_3 \triangleq \|\hat{\mathbf{B}}^H\tilde{\mathbf{a}}_1\|^2$, and $2v_3$ is distributed according to $\chi^2(2n)$. The most harmful position of Eve in this scenario still is $(x^*, y^*) = (-0.5 - \Delta, 0)$. Also, SNR_{AB} in (6) is not affected by the smart jamming from Bob.

A. CDF of S

Assuming $S > 0$, the cumulative distribution function (CDF) of S conditioned on λ_1 is $F_S(s) = \mathcal{P}\{S \leq s|\lambda_1\} = \mathcal{P}\{\log_2(1 + SNR_{AB}) - \log_2(1 + SNR_{AE}) \leq s|\lambda_1\} = \mathcal{P}\{v_1 - W_1 v_2 - W_2 v_3 - W_3 \geq 0|\lambda_1\}$, where

$$W_1 = \frac{(1-\phi)(\frac{\phi\lambda_1 P_A}{1+\rho P_B} - 2^s + 1)}{(L-1)(2^s\phi)}, \tag{22}$$

$$W_2 = \frac{bP_B(\frac{\phi\lambda_1 P_A}{1+\rho P_B} - 2^s + 1)}{n(2^s\phi P_A a)}, \tag{23}$$

$$W_3 = \frac{(\frac{\phi\lambda_1 P_A}{1+\rho P_B} - 2^s + 1)}{(2^s\phi P_A a)}. \tag{24}$$

It follows that

$$F_S(s) = \frac{e^{-W3}}{(1+W_2)^n(1+W_1)^{L-1}(n-1)!\,(L-2)!}$$
$$\times \sum_{k=0}^{N-1}\sum_{i=0}^{k}\sum_{j=0}^{i}\frac{1}{k!}\binom{k}{i}\binom{i}{j}(k-i+L-2)!\,(i-j+n-1)!$$
$$\times \left(\frac{W_1}{1+W_1}\right)^{k-i}\left(\frac{W_2}{1+W_2}\right)^{i-j} W_3^j. \tag{25}$$

Note that for the case of Eve using OMF, a closed form of the CDF of S is not available.

B. Optimization

In order to find the optimal ϕ and P_B, we consider a reference secrecy level s_0 and minimize $F_S(s_0)$. To guarantee some quality of service, we constrain the rate from Alice to Bob not to be less than c. Then our optimization problem is

$$\min_{\phi,\ P_B} \quad F_S(s_0) \tag{26}$$

subject to $0 \leq P_B \leq P_B^{max}$, $0 \leq \phi \leq 1$, and $\phi - \frac{(2^c-1)\rho}{P_A\lambda_1}P_B \geq \frac{(2^c-1)}{P_A\lambda_1}$ which comes from Alice to Bob rate constraint. All these constraints are linear, and hence we can apply the projected gradient descent method. At each step of the gradient descent, the search direction is projected into a direction tangent to the constraints that may be violated by taking the update step.

Unless mentioned otherwise later, assume $N = L = M = 8$, $P_A = 20$ dB, $\rho = 3\times10^{-4}$, $s_0 = 4$, $c = 6$, and $P_B^{max} = 40$ dB. Fig. 3 shows $F_S(s)$ with the optimal and non-optimal ϕ. Fig. 4 shows $F_S(s)$ with the optimal and non-optimal P_B. Fig. 5 compares the averaged secrecy capacity versus P_A against the most harmful Eve using OMF or BMF and using 4, 12, or 90 antennas while Alice and Bob each have 4 antennas. If Eve has the same number of antennas as Alice and Bob and performs OMF, we have considerable secrecy, but if Eve has 3 times that number of antennas ($N = 12$), secrecy decreases substantially, and goes to zero if Eve has more than 20 times that number of antennas ($N = 90$). However, if Eve is unable to use OMF but BMF, there is still a substantial secrecy even for a large number of antennas at Eve. This makes the smart jamming from Bob an important idea. More details will be shown in a full paper.

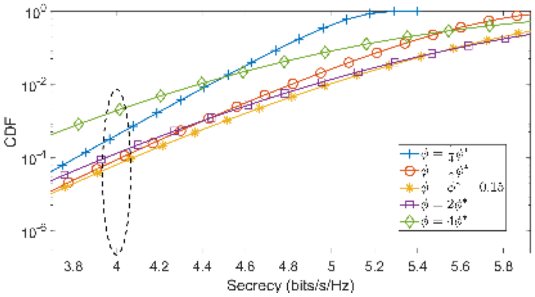

Figure 3: The CDF $F_S(s)$ using optimal $\phi = 0.15$ or non-optimal ϕ with $s_0 = 4$. P_B^* is used for all the curves.

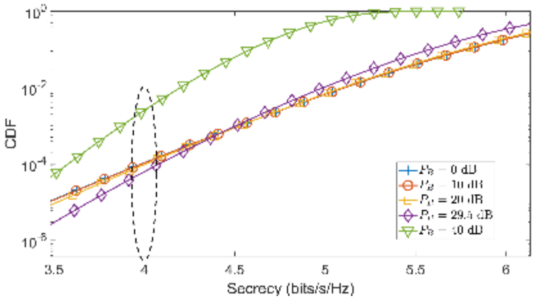

Figure 4: The CDF $F_S(s)$ using optimal $P_B = 29.5$ dB or non-optimal P_B with $s_0 = 4$. ϕ^* is used for all the curves.

V. Conclusion

In this paper, we have examined the secrecy capacity of a MIMO channel from Alice to Bob against multiple-antenna Eves at unknown locations. We have focused on the worst case of Eves who may collude at the network layer (but not at the physical layer) subject to a secured zone around Alice. We have treated two important cases where Eve either uses OMF or BMF, the former of which is not applicable by Eve if Bob uses a smart jamming. For the two cases, different methods are needed, and hence have been developed, to optimize the jamming parameters used by Alice and Bob. Simulation results show significant improvements of the secrecy capacity with the optimized jamming parameters. Future work includes comparison with the anti-eavesdropping channel estimation based approach [12].

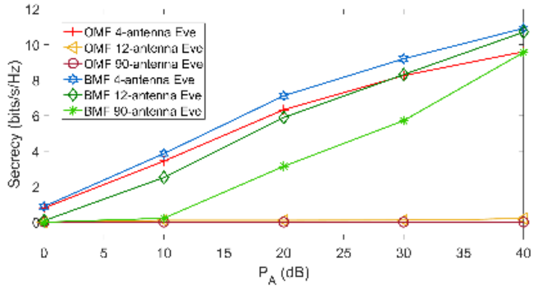

Figure 5: Comparison of averaged secrecy in four scenarios based on N and Eve's filtering method.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[4] ——, "Secure transmission with multiple antennas part ii: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov 2010.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

[6] L. Lai and H. E. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept 2008.

[7] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO gaussian wiretap channel with a cooperative jammer," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 5013–5022, Oct 2011.

[8] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Transactions on Information Theory*, vol. 60, no. 6, pp. 3359–3378, June 2014.

[9] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, no. 3. IEEE; 1999, 2005, p. 1906.

[10] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

[11] Y. Hua, Q. Zhu, and R. Sohrabi, "Fundamental properties of full-duplex radio for secure wireless communications," *arXiv:1711.10001*, 2017.

[12] Y. Hua, "Advanced properties of full-duplex radio for securing wireless network," *IEEE Transactions on Signal Processing*, to appear.

[13] L. Chen, Q. Zhu, W. Meng, and Y. Hua, "Fast power allocation for secure communication with full-duplex radio," *IEEE Transactions on Signal Processing*, vol. 65, no. 14, pp. 3846–3861, 2017.

[14] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Processing Letters*, vol. 21, no. 7, pp. 804–808, 2014.

[15] Y. Zhou, Y. Zhu, and Z. Xue, "Enhanced MIMOME wiretap channel via adopting full-duplex MIMO radios," in *Global Communications Conference (GLOBECOM), 2014 IEEE*. IEEE, 2014, pp. 3320–3325.

[16] O. Cepheli, G. Dartmann, G. K. Kurt, and G. Ascheid, "A joint optimization scheme for artificial noise and transmit filter for half and full duplex wireless cyber physical systems," *IEEE Transactions on Sustainable Computing*, 2017.

[17] O. Cepheli, S. Tedik, and G. K. Kurt, "A high data rate wireless communication system with improved secrecy: Full duplex beamforming," *IEEE communications letters*, vol. 18, no. 6, pp. 1075–1078, 2014.

[18] S. Yun, J. Park, S. Im, and J. Ha, "On the secrecy rate of artificial noise assisted MIMOME channels with full-duplex receiver," in *Wireless Communications and Networking Conference (WCNC), 2017 IEEE*. IEEE, 2017, pp. 1–6.

[19] M. Masood, A. Ghrayeb, P. Babu, I. Khalil, and M. Hasna, "A minorization–maximization algorithm for maximizing the secrecy rate of the MIMOME wiretap channel," *IEEE Communications Letters*, vol. 21, no. 3, pp. 520–523, 2017.

[20] Y. Yang, G. Scutari, D. P. Palomar, and M. Pesavento, "A parallel decomposition method for nonconvex stochastic multi-agent optimization problems," *IEEE Transactions on Signal Processing*, vol. 64, no. 11, pp. 2949–2964, 2016.