electronics

MDPI

Article

Exploiting Array Pattern Synthesis for Physical Layer Security in Millimeter Wave Channels

Jong-Ho Lee [1], Jeongsik Choi [2], Woong-Hee Lee [3] and Jiho Song [4,*]

[1] School of Electronic Engineering, Soongsil University, Seoul 06978, Korea
[2] Intel Labs, Intel Corporation, Santa Clara, CA 95054-1549, USA
[3] Department of Communication Systems, KTH Royal Institute of Technology, 114 28 Stockholm, Sweden
[4] School of Electrical Engineering, University of Ulsan, Ulsan 44610, Korea
* Correspondence: jihosong@ulsan.ac.kr; Tel.: +82-52-259-2211

Received: 12 June 2019; Accepted: 27 June 2019; Published: 1 July 2019

Abstract: In this paper, we propose a beamformer design scheme for wireless physical layer security using partial channel state information (CSI) in millimeter wave channels. The partial CSI used in this work is the range of angle-of-departure (AOD). Assuming that the AOD range of each node is available, we design a transmit beamformer using semidefinite programming based on array pattern synthesis. Numerical results are presented to verify the secrecy rates achieved by the proposed scheme.

Keywords: physical layer security; array pattern synthesis; beamforming; semidefinite programming

1. Introduction

One inherent defect in wireless communication systems is their lack of security owing to the broadcast nature of wireless channels. To enable secure transmission over wireless channels, physical layer security schemes exploit the physical characteristics of wireless channels without relying on cryptography [1,2]. From an information-theoretic viewpoint, secrecy capacity is defined as the maximum achievable secrecy rate at which a source can send a confidential message to a destination without being overheard by eavesdroppers. To enlarge the secrecy rate in wireless channels, various approaches have been studied to exploit multiple-antenna techniques [3,4], relay-assisted secure transmission schemes [5], node cooperation strategies [6–8], and dirty paper coding (DPC) based information embedding approaches [9], where global channel state information (CSI) is assumed. In [10,11], secure communication with delayed CSI has been investigated from a secure degrees of freedom perspective.

To enhance wireless physical layer security even when global CSI is not available, beamforming with artificial noise has been widely investigated [12,13]. In [14], the artificial noise is placed in the null space of the destination's channel to prevent artificial noise from leaking to the destination. Further, to decide what portion of available transmit power is allocated for sending artificial noise to interrupt eavesdroppers, the statistics of the eavesdroppers' channels are exploited at the source in [15]. Since the exact CSI of the destination's channel is required for the above techniques, the leakage of artificial noise to the destination is inevitable when the destination's channel estimation is imperfect [16].

In this work, we propose a beamformer design scheme exploiting partial CSI in millimeter wave (mmWave) channels. The partial CSI exploited in this work is the range of angle-of-departure (AOD). We assume that even though the AOD of a dominant multipath between the BS and each node is not exactly known to the BS, it falls within a certain range and the AOD ranges of the destination and the eavesdroppers are available at the BS. Note that compound wiretap channels in [17] assume that the destination's channel is perfectly known, while the eavesdroppers' channels belong to a known set of channels characterized by partial CSI such as maximum channel gain. The AOD ranges for the eavesdroppers in this work can be considered as the known set of channels defined in compound wiretap channels. While the compound wiretap channel assumes the perfect knowledge on the destination's channel, we consider only the AOD range for the destination. Using the AOD range information, we design a transmit beamformer for sending confidential messages based on array pattern synthesis using semidefinite programming [18].

Recently, array pattern synthesis has been utilized to design cluster beamformers in non-orthogonal multiple access systems. In [19], the cluster beamformer is designed to minimize inter-cluster interference under the constraint of maintaining the beamforming gain to the desired cluster exceeding a given threshold. Unlike the previous study in [19], we focus on maximizing the ratio of the beamforming gains at the destination and the eavesdroppers by considering that the secrecy rate is determined by the difference between rates at the destination and the eavesdroppers. Using numerical results, we show that the proposed approach using AOD ranges is efficient for physical layer security when the array antenna size is large and the channel estimation error is critical.

2. System Model and Secrecy Rate Evaluation

Consider a BS that sends secure information to a destination in the presence of I non-colluding eavesdroppers [20]. In a non-colluding scenario, each eavesdropper works independently and decodes the message solely based on its own observation. On the other hand, a colluding scenario considers that multiple eavesdroppers share their observations and jointly decode the message assuming the existence of communication links between eavesdroppers, which represents a worst-case scenario. The colluding eavesdroppers can be treated as a single eavesdropper with multiple antennas in [3]. Even though we propose a beamformer design scheme assuming non-colluding eavesdroppers, the secrecy rate achieved by the proposed beamformer is also evaluated in a colluding scenario, which will be presented in Section 4.

We assume that the BS has an antenna array with N antenna elements, whereas the destination D and each eavesdropper E_i are equipped with a single antenna. Let y_D and y_{E_i} be the received baseband signals at D and E_i, respectively. The received signals can be expressed as

$$\begin{aligned} y_D &= \mathbf{h}_D \mathbf{w} s + z_D, \\ y_{E_i} &= \mathbf{h}_{E_i} \mathbf{w} s + z_{E_i}, \end{aligned} \tag{1}$$

where $\mathbf{h}_D \in \mathbb{C}^{1\times N}$ and $\mathbf{h}_{E_i} \in \mathbb{C}^{1\times N}$ are vectors containing the complex channel coefficients from the BS to D and E_i, respectively. Further, $\mathbf{w} = [w_1\ w_2\ \cdots\ w_N]^T \in \mathbb{C}^N$ denotes a transmit beamformer and s is the secure information with unit power. The noises z_D and z_{E_i} are assumed to be complex additive white Gaussian with zero-mean and variance σ^2. Here, we can compute the rates at D and E_i as

$$\begin{aligned} \mathcal{R}_D &= \log_2\left(1 + \frac{|\mathbf{h}_D \mathbf{w}|^2}{\sigma^2}\right), \\ \mathcal{R}_{E_i} &= \log_2\left(1 + \frac{|\mathbf{h}_{E_i} \mathbf{w}|^2}{\sigma^2}\right), \end{aligned} \tag{2}$$

respectively. Then, the achievable secrecy rate can be expressed as $\mathcal{R} = \max\left\{\mathcal{R}_D - \max_i \mathcal{R}_{E_i}, 0\right\}$ [21].

Assuming global CSI is available at the BS, we can find the optimal transmit beamformer, which maximizes the achievable secrecy rate, by solving the following optimization problem:

$$\max_{\mathbf{w}} \frac{\sigma^2 + |\mathbf{h}_D \mathbf{w}|^2}{\max_i \left\{\sigma^2 + |\mathbf{h}_{E_i} \mathbf{w}|^2\right\}}, \quad \text{s.t. } \mathbf{w}^\dagger \mathbf{w} = P, \tag{3}$$

where $(.)^\dagger$ denotes the conjugated transpose and P is the transmit power of the BS. The detailed derivation for solving (3) is highlighted in the Appendix. It is noteworthy that the beamformer design problem to minimize the transmit power with the secrecy rate constraint is also considered in [21].

Let us consider a uniform planar array (UPA) at the BS, where N antenna elements are placed in a two-dimensional grid pattern. When channel reciprocity is available, the channels from the BS to D and E_i can be expressed as [22]

$$\mathbf{h}_D = \left(\mathbf{A}_D \mathbf{g}_D\right)^\dagger, \; \mathbf{h}_{E_i} = \left(\mathbf{A}_{E_i} \mathbf{g}_{E_i}\right)^\dagger, \tag{4}$$

respectively, where $\mathbf{g}_D \in \mathbb{C}^{K_D}$ and $\mathbf{g}_{E_i} \in \mathbb{C}^{K_{E_i}}$ are complex Gaussian vectors with zero mean and covariance matrices $\mathrm{diag}(\beta_D^{(1)}, \cdots, \beta_D^{(K_D)})$ and $\mathrm{diag}(\beta_{E_i}^{(1)}, \cdots, \beta_{E_i}^{(K_{E_i})})$, respectively. Furthermore, K_D denotes the number of multipaths between the BS and D, K_{E_i} is the number of multipaths between the BS and E_i, and $\beta_D^{(k)}$ and $\beta_{E_i}^{(k)}$ denote the average power gain for each radio path. The k-th columns of the matrix $\mathbf{A}_D \in \mathbb{C}^{N \times K_D}$ and the matrix $\mathbf{A}_{E_i} \in \mathbb{C}^{N \times K_{E_i}}$ are given as the steering vectors $\mathbf{a}_D^{(k)}$ and $\mathbf{a}_{E_i}^{(k)}$, respectively. Here, the n-th entries of $\mathbf{a}_D^{(k)}$ and $\mathbf{a}_{E_i}^{(k)}$ are defined as $\frac{1}{\sqrt{K_D}} e^{j2\pi\left(u_D^{(k)} x_n + v_D^{(k)} y_n\right)}$ and $\frac{1}{\sqrt{K_{E_i}}} e^{j2\pi\left(u_{E_i}^{(k)} x_n + v_{E_i}^{(k)} y_n\right)}$, respectively, where x_n and y_n denote the location of the n-th antenna element in wavelengths, which can be arbitrary but fixed and known, and

$$\begin{aligned} u_D^{(k)} &= \sin(\theta_D^{(k)}) \cos(\varphi_D^{(k)}), \;\; v_D^{(k)} = \sin(\theta_D^{(k)}) \sin(\varphi_D^{(k)}), \\ u_{E_i}^{(k)} &= \sin(\theta_{E_i}^{(k)}) \cos(\varphi_{E_i}^{(k)}), \;\; v_{E_i}^{(k)} = \sin(\theta_{E_i}^{(k)}) \sin(\varphi_{E_i}^{(k)}). \end{aligned} \tag{5}$$

Here, $(\theta_D^{(k)}, \varphi_D^{(k)})$ and $(\theta_{E_i}^{(k)}, \varphi_{E_i}^{(k)})$ denote the AOD of the k-th multipath from D to the BS and from E_i to the BS, respectively.

Considering the directional characteristics of mmWave channels and their poor scattering environments [23], we assume that $(u_D^{(1)}, v_D^{(1)})$ and $(u_{E_i}^{(1)}, v_{E_i}^{(1)})$ for dominant radio paths are within certain AOD regions S_D and S_{E_i} in the horizontal and vertical (u-v) domain, respectively, and S_D and $S_E = \cup_{i=1}^{I} S_{E_i}$ are mutually exclusive. The AODs of the other multipaths, which are much weaker than the dominant multipath, are assumed to be unknown and distributed randomly in the u-v domain.

3. Secrecy Rate Maximization via Array Pattern Synthesis

Our approach to designing $\mathbf{w}$ with S_D and S_E is based on antenna pattern nulling to maximize the ratio between the minimum radiation to S_D and the maximum radiation to S_E. Considering only the dominant radio path, we approximate the objective function in (3) as $\frac{\sigma^2 + \beta_D^{(1)} |\mathbf{a}_D^{(1)} \mathbf{w}|^2}{\max_i \left\{\sigma^2 + \beta_{E_i}^{(1)} |\mathbf{a}_{E_i}^{(1)} \mathbf{w}|^2\right\}}$. Note that $\mathbf{a}_D^{(1)}$ and $\mathbf{a}_{E_i}^{(1)}$ can be determined only when $(u_D^{(1)}, v_D^{(1)})$ and $(u_{E_i}^{(1)}, v_{E_i}^{(1)})$ are given. Since only the partial CSI S_D and S_E are available, we assume that the average power gain for the dominant radio path to noise ratio is the same for D and E_i (i.e., $\frac{\beta_D^{(1)}}{\sigma^2} = \frac{\beta_{E_i}^{(1)}}{\sigma^2} = \frac{1}{\check{\sigma}^2}$) and consider a worst-case scenario given as

$$\max_{\mathbf{w}} \frac{\min\limits_{(u,v)\in S_D} \; \check{\sigma}^2 + \mathbf{w}^\dagger \mathbf{\Gamma}(u,v) \mathbf{w}}{\max\limits_{(u,v)\in S_E} \; \check{\sigma}^2 + \mathbf{w}^\dagger \mathbf{\Gamma}(u,v) \mathbf{w}}, \quad \text{s.t. } \mathbf{w}^\dagger \mathbf{w} = P, \tag{6}$$

where $\mathbf{\Gamma}(u,v) = \mathbf{a}(u,v)\mathbf{a}(u,v)^\dagger$ and the n-th entry of the steering vector $\mathbf{a}(u,v) \in \mathbb{C}^N$ is given as $e^{j2\pi(ux_n + vy_n)}$. Let us rewrite (6) as

$$\max_{\mathbf{w}} \frac{\min\limits_{(u,v)\in S_D} \; \mathbf{w}^\dagger \tilde{\mathbf{\Gamma}}(u,v) \mathbf{w}}{\max\limits_{(u,v)\in S_E} \; \mathbf{w}^\dagger \tilde{\mathbf{\Gamma}}(u,v) \mathbf{w}}, \quad \text{s.t. } \mathbf{w}^\dagger \mathbf{w} = P, \tag{7}$$

where $\tilde{\mathbf{\Gamma}}(u,v) = \mathbf{I}_N + \frac{P}{\tilde{\sigma}^2}\mathbf{\Gamma}(u,v)$. Note that (7) can be rewritten as

$$\begin{aligned} \max_{\mathbf{w},\tau_D,\tau_E} \quad & \frac{\tau_D}{\tau_E} \\ \text{s.t.} \quad & \mathbf{w}^\dagger \tilde{\mathbf{\Gamma}}(u,v)\mathbf{w} \geq \tau_D,\ \forall(u,v) \in S_D, \\ & \mathbf{w}^\dagger \tilde{\mathbf{\Gamma}}(u,v)\mathbf{w} \leq \tau_E,\ \forall(u,v) \in S_E, \\ & \mathbf{w}^\dagger \mathbf{w} = P. \end{aligned} \tag{8}$$

It is obvious that (8) is equivalent to

$$\begin{aligned} \max_{\mathbf{W},\tau_D,\tau_E,\rho} \quad & \rho \\ \text{s.t.} \quad & \text{tr}(\tilde{\mathbf{\Gamma}}(u,v)\mathbf{W}) \geq \tau_D,\ \forall(u,v) \in S_D, \\ & \text{tr}(\tilde{\mathbf{\Gamma}}(u,v)\mathbf{W}) \leq \tau_E,\ \forall(u,v) \in S_E, \\ & \tau_D - \rho\tau_E = 0, \\ & \text{tr}(\mathbf{W}) = P,\ \mathbf{W} \succeq 0,\ \text{rank}(\mathbf{W}) = 1, \end{aligned} \tag{9}$$

where $\mathbf{W} = \mathbf{w}\mathbf{w}^\dagger$, tr(.) denotes the trace operation, and $\mathbf{W} \succeq 0$ indicates that $\mathbf{W}$ is a Hermitian positive semidefinite matrix.

To solve (9), we first ignore the rank constraint based on semidefinite relaxation [24]. Then, the problem becomes quasi-convex. It is noteworthy that all the inequality constraints in (9) are convex [25]. We can solve this quasi-convex problem using the bisection technique [25,26]. In detail, let us first consider the following convex feasibility problem for any given value of ρ:

$$\begin{aligned} \text{find} \quad & \mathbf{W}, \tau_D, \tau_E \\ \text{such that} \quad & \text{tr}(\tilde{\mathbf{\Gamma}}(u,v)\mathbf{W}) \geq \tau_D,\ \forall(u,v) \in S_D, \\ & \text{tr}(\tilde{\mathbf{\Gamma}}(u,v)\mathbf{W}) \leq \tau_E,\ \forall(u,v) \in S_E, \\ & \tau_D - \rho\tau_E = 0,\ \text{tr}(\mathbf{W}) = P,\ \mathbf{W} \succeq 0. \end{aligned} \tag{10}$$

By using a semidefinite program solver such as SeDuMi [27] and Yalmip [28], we can check the feasibility of (10). The infeasibility of (10) indicates that the given ρ cannot be achieved, even though we ignored the rank constraint. Then, we conclude that the maximum value of ρ, denoted as ρ_{max}, is less than the given ρ [26]. If (10) is feasible and the solution of (10), denoted as $\mathbf{W}^\star$, $\tau_D^\star$, and $\tau_E^\star$, can be obtained, we should confirm that $\mathbf{W}^\star$ is of rank one because the rank constraint is ignored in our problem. When $\mathbf{W}^\star$ is of rank one, the given ρ can be achieved with the principal eigenvector of $\mathbf{W}^\star$. In this case, we conclude that $\rho_{max} \geq \rho$.

If the rank of $\mathbf{W}^\star$ is higher than one, we have to determine whether any other rank-one solution to achieve the given ρ exists or not. Here, the penalty function method (PFM) in [7] is adopted. Using $\mathbf{W}^\star$, $\tau_D^\star$, and $\tau_E^\star$, we first set $\mathbf{W}'^{(0)} = \mathbf{W}^\star$ and perform the initialization step of the PFM. The initialization step of the PFM can provide $\mathbf{W}^{(0)}$ with rank$(\mathbf{W}^{(0)}) \approx 1$. Then, $\mathbf{W}^{(0)}$ is used as a starting point for the optimization step of the PFM. Both the initialization and optimization steps are iterative processes. At the j-th iteration, both steps solve the following semidefinite programming problem:

$$\begin{aligned} \mathbf{W}^{(j+1)} \quad & = \underset{\tilde{\mathbf{W}}}{\text{argmin}}\ \text{tr}(\tilde{\mathbf{W}}) - \lambda_{max}(\mathbf{W}^{(j)}) - \text{tr}(\mathbf{w}_{max}^{(j)}(\mathbf{w}_{max}^{(j)})^\dagger(\tilde{\mathbf{W}} - \mathbf{W}^{(j)})) \\ \text{s.t.} \quad & \text{tr}(\tilde{\mathbf{\Gamma}}(u,v)\tilde{\mathbf{W}}) \geq \tau_D^\star,\ \forall(u,v) \in S_D, \\ & \text{tr}(\tilde{\mathbf{\Gamma}}(u,v)\tilde{\mathbf{W}}) \leq \tau_E^\star,\ \forall(u,v) \in S_E, \\ & \text{tr}(\tilde{\mathbf{W}}) = P,\ \tilde{\mathbf{W}} \succeq 0, \end{aligned} \tag{11}$$

where $\lambda_{max}(\mathbf{W}^{(j)})$ and $\mathbf{w}_{max}^{(j)}$ are the maximum eigenvalue and the corresponding eigenvector of $\mathbf{W}^{(j)}$. If we obtain a rank-one solution via the PFM for the given ρ, we conclude that $\rho_{max} \geq \rho$. When a rank-one solution is not available even though the PFM is performed, we conclude $\rho_{max} < \rho$.

Using the above results, we exploit the bisection technique with the initial interval $[L, U]$, which is assumed to include ρ_{max}. At the midpoint of the interval $\rho = \frac{L+U}{2}$, (10) is solved as we described above. If it is infeasible, we update the upper bound of the interval as $U = \rho$. If it is feasible, we confirm whether the rank of $\mathbf{W}^\star$ is one or not. The lower bound of the interval is updated as $L = \rho$ when $\mathbf{W}^\star$ is of rank one. Otherwise, the PFM is performed whether a rank-one solution for the given ρ exists or not. If the solution provided by the PFM is of rank one, the lower bound of the interval is updated as $L = \rho$. Otherwise, we update $U = \rho$. The above process is performed again for the updated interval, until the width of the interval is small enough (i.e., $U - L \leq \epsilon_b$, where ϵ_b is the desired accuracy). Since the initial interval is halved at each iteration, $\lceil \log_2((U-L)/\epsilon_b) \rceil$ iterations are required [29]. As commented in [7], we also found that the above process can always provide a rank-one solution in our simulations.

For numerical implementations, the constraints $\mathrm{tr}(\tilde{\mathbf{\Gamma}}(u,v)\mathbf{W}) \geq \tau_D$, $\forall (u,v) \in S_D$ and $\mathrm{tr}(\tilde{\mathbf{\Gamma}}(u,v)\mathbf{W}) \leq \tau_E$, $\forall (u,v) \in S_E$ in (10) are approximated as

$$\begin{aligned} \mathrm{tr}(\tilde{\mathbf{\Gamma}}(u_p,v_p)\mathbf{W}) &\geq \tau_D, \ \forall p, \\ \mathrm{tr}(\tilde{\mathbf{\Gamma}}(u_q,v_q)\mathbf{W}) &\leq \tau_E, \ \forall q, \end{aligned} \tag{12}$$

where (u_p, v_p) and (u_q, v_q) denote the sample points in S_D and S_E, respectively [30]. When the numbers of the sample points in S_D and S_E are given as Q_D and Q_E, we have to solve (10) with a matrix variable of size $N \times N$, 2 nonnegative variables, and $Q_D + Q_E + 2$ linear constraints at each iteration of the bisection process. Interior point methods will take $O\left(\sqrt{N+2}\log(1/\epsilon)\right)$ iterations, where ϵ represents the solution accuracy at the algorithm's termination, and each iteration requires at most $O\left((N+2)^6 + (Q_D+Q_E+2)(N+2)^2\right)$ arithmetic operations [29]. Further, at each iteration of the PFM, we solve (11), which will take $O\left(\sqrt{N}\log(1/\epsilon)\right)$ iterations and each iteration requires at most $O\left(N^6 + (Q_D+Q_E+1)N^2\right)$ arithmetic operations [7].

4. Numerical Evaluation

In this section, we present numerical results to verify the secrecy rate performance of the proposed scheme. For simulation simplicity, we assume that S_D is a circle in the u-v domain given as

$$S_D = \{(u,v); (u-u_D)^2 + (v-v_D)^2 < r_D^2\}, \tag{13}$$

where (u_D, v_D) and r_D are the center and the radius of the circle, respectively. For each channel realization, $(u_D^{(1)}, v_D^{(1)})$ for a dominant path is randomly chosen within S_D, while $(u_D^{(k)}, v_D^{(k)})$ with $k = 2, \cdots, K_D$ are randomly chosen in the whole u-v domain. S_{E_i} is also assumed to be a circle in the u-v domain with a center of (u_{E_i}, v_{E_i}) and radius of r_{E_i}. $(u_{E_i}^{(1)}, v_{E_i}^{(1)})$ is randomly chosen within S_{E_i}, while $(u_{E_i}^{(k)}, v_{E_i}^{(k)})$ with $k = 2, \cdots, K_{E_i}$ are randomly chosen in the whole u-v domain. Note that the proposed scheme can be adopted for arbitrary shapes of S_D and S_{E_i}.

In the following results, we fix $P = 1$, $r_D = r_{E_i} = 0.1$, $\sigma^2 = 10^{-3}$, and $K_D = K_{E_i} = K$. Without loss of generality, we set $u_D = v_D = 0$ and consider a UPA with $\tilde{N} \times \tilde{N}$ antenna elements (i.e., $N = \tilde{N}^2$), where each element is uniformly spaced by half a wavelength. The far field radiated by the planar array can be expressed as $f(u,v) = \sum_{n=1}^{N} r_n(u,v) w_n e^{j2\pi(ux_n + vy_n)}$ [30], where $r_n(u,v)$ is the radiation pattern of the n-th antenna element. The n-th antenna element is fed by w_n, which denotes the n-th entry of $\mathbf{w}$. In our simulation, we assume isotropic antenna elements with $r_n(u,v) = 1$ [30]. Let us refer to $|f(u,v)|^2$ as the beamforming gain of the antenna array.

Let us consider a scenario where $I = 6$ eavesdroppers exist in the network and each (u_{E_i}, v_{E_i}) is given as in Table 1. Here, we verify the validity of the proposed beamformer from the viewpoint of the beamforming gain of the planar array. For illustration purposes, we present the beamforming gain of the transmit beamformer obtained by the proposed scheme for this scenario when $\tilde{N} = 8$ in

Figure 1. The interior of the black circle is S_D, whereas the interior of the white circle denotes S_{E_i}. We found that the proposed beamformer provides 12.58 dB of the minimum beamforming gain in S_D and −33.77 dB of the maximum beamforming gain in S_E. From the simulation results, we found that the ratio between the minimum beamforming gain in S_D and the maximum beamforming gain in S_E increases with increasing $\tilde{N}$.

Table 1. The center of the circle for E in the u-v domain.

i	(u_{E_i}, v_{E_i})
1	(0.3,0.7)
2	(−0.4,−0.5)
3	(0.5,−0.2)
4	(−0.8,0.3)
5	(0.3,−0.3)
6	(0.9,0.1)

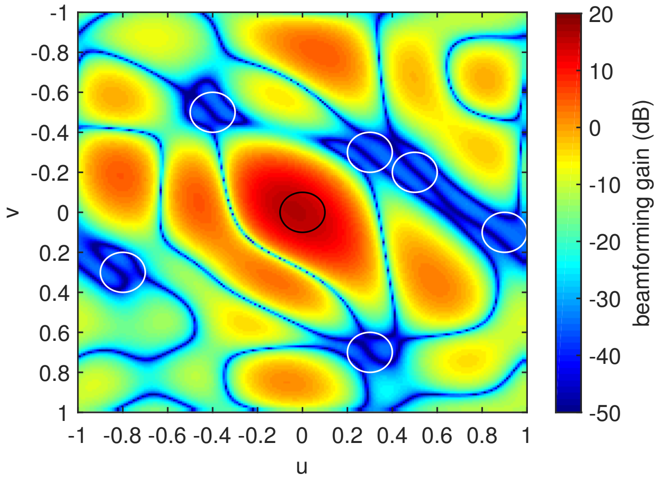

Figure 1. Beamforming gain of the proposed beamformer when $\tilde{N} = 8$.

In Appendix A, we derived the transmit beamformer for global CSI. Further, to investigate the impact of imperfect CSI, we assumed that the imperfect channel coefficients $\hat{\mathbf{h}}_D$ and $\hat{\mathbf{h}}_{E_i}$ are used instead of the exact channel coefficients $\mathbf{h}_D$ and $\mathbf{h}_{E_i}$, where $\hat{\mathbf{h}}_D = \mathbf{h}_D + \mathbf{v}_D$ and $\hat{\mathbf{h}}_{E_i} = \mathbf{h}_{E_i} + \mathbf{v}_{E_i}$, respectively. Here, each entry of $\mathbf{v}_D$ and $\mathbf{v}_{E_i}$ is assumed to be independent and identically distributed complex Gaussian with zero mean and ζ^2 variance. We computed the transmit beamformer as in the Appendix A by replacing $\mathbf{h}_D$ and $\mathbf{h}_{E_i}$ with the imperfect CSI $\hat{\mathbf{h}}_D$ and $\hat{\mathbf{h}}_{E_i}$, respectively.

In Figure 2, we compare the secrecy rate achieved by the proposed scheme and that with imperfect CSI for different values of $\tilde{N}$. We set $K = 3$ and consider that $\beta_D^{(1)} = \beta_{E_i}^{(1)} = 1$, $\beta_D^{(2)} = \beta_{E_i}^{(2)} = 0.1$, and $\beta_D^{(3)} = \beta_{E_i}^{(3)} = 0.0316$, which indicate that the second and third multipaths are 10 dB and 15 dB weaker than the dominant multipath, respectively [23]. $\zeta^2 = 0$ indicates the exact CSI. As expected, the secrecy rate for imperfect CSI decreases with an increase of ζ^2. Note that the secrecy rate performance of the proposed scheme is independent of ζ^2. It is observed that ζ^2 at which the secrecy rate with imperfect CSI is better than that of the proposed scheme decreases as $\tilde{N}$ increases. This indicates that the proposed scheme is efficient when the size of the antenna array is large and the channel estimation error becomes critical.

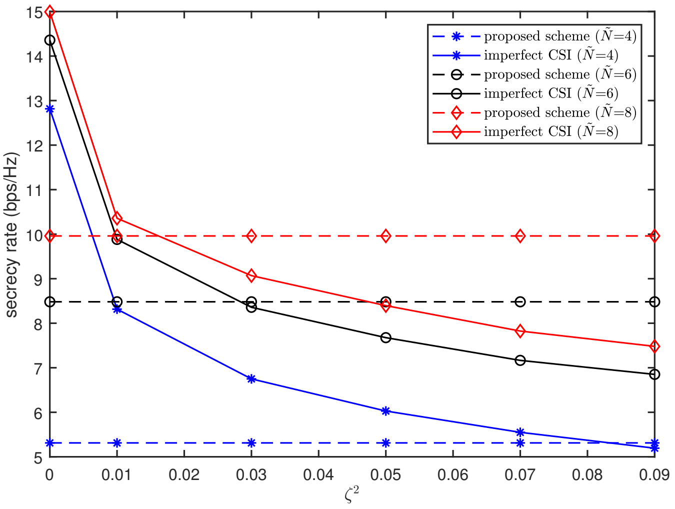

Figure 2. Comparison of secrecy rates as a function of ζ^2.

As described above, we consider that only the dominant path is within the given AOD region and the other multipaths are randomly distributed. It is expected that the other multipaths with AODs outside the given AOD region degrade the secrecy rate performance of the proposed scheme. In order to investigate the impact of the other multipaths, we evaluate the secrecy rate of the proposed scheme for different numbers of multipaths as shown in Figure 3. For $K = 1$, we consider only the dominant path with $\beta_D^{(1)} = \beta_{E_i}^{(1)} = 1$, whose AOD is within the given AOD region. Note that $K = 1$ is optimal for the proposed scheme. For $K = 2$, the second path is added with $\beta_D^{(2)} = \beta_{E_i}^{(2)} = 0.1$, which is 10 dB weaker than the dominant path. For $K = 3$, we use the same setting for $\beta_D^{(k)}$ and $\beta_{E_i}^{(k)}$ as in Figure 2. When $K \geq 4$, we add the multipaths which are 15 dB weaker than the dominant path. As expected, the secrecy rate performance of the proposed scheme degrades with an increase of K. In particular, the gap between the secrecy rates with $K = 1$ and 2 is remarkable. For $\tilde{N} = 8$, it is found that the secrecy rate with $K = 2$ is about 76% of that with $K = 1$. However, the secrecy rate is shown to decrease slightly when $K \geq 2$.

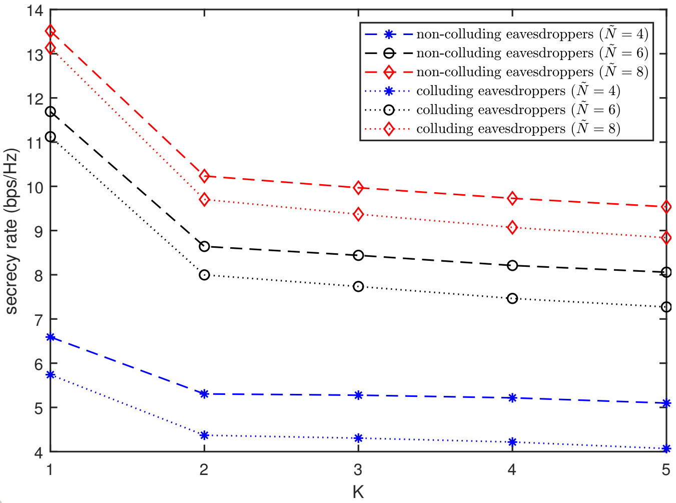

Figure 3. Secrecy rate comparison of the proposed scheme in non-colluding and colluding scenarios as a function of K.

Figure 3 also presents the secrecy rate achieved by the proposed scheme in a colluding scenario. The rate at the colluding eavesdroppers can be given as $\mathcal{R}_E = \log_2\left(1 + \frac{||\mathbf{H}_E\mathbf{w}||^2}{\sigma^2}\right)$, where $\mathbf{H}_E = [\mathbf{h}_{E_1}^T\ \mathbf{h}_{E_2}^T\ \cdots\ \mathbf{h}_{E_I}^T]^T$ [3] and the achievable secrecy rate is computed as $\mathcal{R} = \max\{\mathcal{R}_D - \mathcal{R}_E, 0\}$. Since the proposed beamformer minimizes the beamforming gains to all eavesdroppers as shown in Figure 1, the proposed scheme is also effective in a colluding scenario. In Figure 3, the secrecy rate in a colluding scenario is observed to be worse than that in a non-colluding scenario. However, it is noteworthy that the gap between them reduces as $\tilde{N}$ increases.

5. Conclusions

In this paper, we proposed a transmit beamfomer design scheme exploiting partial CSI for physical layer security in mmWave channels. Assuming that the AOD region of each node is available, we designed a transmit beamformer to maximize the ratios between the minimum beamforming gain to the AOD region of the destination and the maximum beamforming gain to the union of the AOD regions of the eavesdroppers. In the numerical results, we compared the secrecy rate achieved by the proposed scheme and that with imperfect CSI to verify the efficiency of the proposed scheme.

Author Contributions: Conceptualization, J.-H.L.; methodology, J.-H.L., J.C. and W.-H.L.; software, J.-H.L.; validation, J.C., W.-H.L. and J.S.; writing—original draft preparation, J.-H.L. and J.S.; writing—review and editing, J.-H.L. and J.S.

Funding: This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(NRF-2016R1D1A1B03930599).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Let us rewrite the optimization problem in (3) to maximize the secrecy rate with global CSI as

$$\max_{\tilde{\mathbf{w}}} \frac{\tilde{\mathbf{w}}^{\dagger}\tilde{\mathbf{R}}_D\tilde{\mathbf{w}}}{\max_i \tilde{\mathbf{w}}^{\dagger}\tilde{\mathbf{R}}_{E_i}\tilde{\mathbf{w}}}, \quad \text{s.t. } \tilde{\mathbf{w}}^{\dagger}\tilde{\mathbf{w}} = 1, \tag{A1}$$

where $\tilde{\mathbf{w}} = \frac{1}{\sqrt{P}}\mathbf{w}$, $\tilde{\mathbf{R}}_D = \frac{\sigma^2}{P}\mathbf{I} + \mathbf{h}_D\mathbf{h}_D^{\dagger}$, and $\tilde{\mathbf{R}}_{E_i} = \frac{\sigma^2}{P}\mathbf{I} + \mathbf{h}_{E_i}\mathbf{h}_{E_i}^{\dagger}$. Note that (A1) is equivalent to

$$\begin{array}{ll} \max\limits_{\tilde{\mathbf{W}}} & \frac{\mathrm{tr}\left(\tilde{\mathbf{R}}_D\tilde{\mathbf{W}}\right)}{\max_i \mathrm{tr}\left(\tilde{\mathbf{R}}_{E_i}\tilde{\mathbf{W}}\right)} \\ \text{s.t.} & \mathrm{tr}\left(\tilde{\mathbf{W}}\right) = 1,\ \mathbf{W} \succeq 0,\ \mathrm{rank}\left(\tilde{\mathbf{W}}\right) = 1. \end{array} \tag{A2}$$

Further, (A2) can be rewritten as

$$\begin{array}{ll} \max\limits_{\tilde{\mathbf{W}},\tau_D,\tau_E} & \frac{\tau_D}{\tau_E} \\ \text{s.t.} & \mathrm{tr}\left(\tilde{\mathbf{R}}_D\tilde{\mathbf{W}}\right) = \tau_D, \\ & \mathrm{tr}\left(\tilde{\mathbf{R}}_{E_i}\tilde{\mathbf{W}}\right) \le \tau_E,\ \forall i, \\ & \mathrm{tr}\left(\tilde{\mathbf{W}}\right) = 1,\ \mathbf{W} \succeq 0,\ \mathrm{rank}\left(\tilde{\mathbf{W}}\right) = 1. \end{array} \tag{A3}$$

Note that (A3) is equivalent to

$$\begin{array}{ll} \max\limits_{\tilde{\mathbf{W}},\rho,\tau_D,\tau_E} & \rho \\ \text{s.t.} & \mathrm{tr}(\tilde{\mathbf{R}}_D\tilde{\mathbf{W}}) = \tau_D, \\ & \mathrm{tr}(\tilde{\mathbf{R}}_{E_i}\tilde{\mathbf{W}}) \le \tau_E, \forall i, \\ & \rho\tau_D = \tau_E,\ \mathrm{tr}(\tilde{\mathbf{W}}) = 1, \\ & \tilde{\mathbf{W}} \succeq 0, \mathrm{rank}(\tilde{\mathbf{W}}) = 1. \end{array} \tag{A4}$$

As in Section 3, we exploit the semidefinite relaxation and use the bisection technique with the PFM. The feasibility problem for this case is given as

$$\begin{aligned} \text{find} \quad & \tilde{\mathbf{W}}, \tau_D, \tau_E \\ \text{such that} \quad & \operatorname{tr}(\tilde{\mathbf{R}}_D \tilde{\mathbf{W}}) = \tau_D, \\ & \operatorname{tr}(\tilde{\mathbf{R}}_{E_i} \tilde{\mathbf{W}}) \leq \tau_E, \ \forall i, \\ & \rho \tau_D = \tau_E, \operatorname{tr}(\tilde{\mathbf{W}}) = 1, \\ & \tilde{\mathbf{W}} \succeq 0. \end{aligned} \tag{A5}$$

References

1. Shiu, Y.S.; Chang, S.Y.; Wu, H.C.; Huang, S.-H.; Chen, H.-H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74. [CrossRef]
2. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573. [CrossRef]
3. Khisti, A.; Wornell, G.W. Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Trans. Inf. Theory* **2010**, *56*, 3088–3104. [CrossRef]
4. Khisti, A.; Wornell, G.W. Secure transmission with multiple antennas II: The MIMOME wiretap channel. *IEEE Trans. Inf. Theory* **2010**, *56*, 5515–5532. [CrossRef]
5. Awan, Z.H.; Zaidi, A.; Vandendorpe, L. Secure communication over parallel relay channel. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 359–371. [CrossRef]
6. Li, J.; Petropulu, A.P.; Weber, S. On cooperative relaying schemes for wireless physical layer security. *IEEE Trans. Signal Process.* **2011**, *59*, 4985–4997. [CrossRef]
7. Wang, H.-M.; Luo, M.; Yin, Q.; Xia, X.-G. Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 2007–2020. [CrossRef]
8. Lee, J.-H. Optimal power allocation for physical layer security in multi-hop DF relay networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 28–38. [CrossRef]
9. Zaidi, A.; Vandendorpe, L. Coding schemes for relay-assisted information embedding. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 70–85. [CrossRef]
10. Zaidi, A.; Awan, Z.H.; Shamai, S.; Vandendorpe, L. Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSIT. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1760–1774. [CrossRef]
11. Awan, Z.H.; Zaidi, A.; Sezgin, A. On SDoF of multi-receiver wiretap channel with alternating CSIT. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1780–1795. [CrossRef]
12. He, B.; Zhou, X.; Abhayapala, T.D. Wireless physical layer security with imperfect channel state information: A survey. *arXiv* **2013**, arXiv:1307.4146v2.
13. Cumanan, K.; Xing, H.; Xu, P.; Zheng, G.; Dai, X.; Nallanathan, A.; Ding, Z.; Karagiannidis, G.K. Physical layer security jamming: Theoretical limits and practical designs in wireless networks. *IEEE Access* **2017**, *5*, 3603–3611. [CrossRef]
14. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
15. Huang, J.; Swindlehurst, A.L. Robust secure transmission in MISO channels based on worst-case optimization. *IEEE Trans. Signal Process.* **2012**, *60*, 1696–1707. [CrossRef]
16. Mukherjee, A.; Swindlehurst, A.L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Trans. Signal Process.* **2011**, *59*, 351–361. [CrossRef]
17. Schaefer, R.F.; Loyka, S. The secrecy capacity of compound Gaussian MIMO wiretap channels. *IEEE Trans. Inf. Theory* **2015**, *61*, 5535–5552. [CrossRef]
18. Fuchs, B. Application of convex relaxation to array synthesis problems. *IEEE Trans. Antennas Propag.* **2014**, *62*, 634–640. [CrossRef]
19. Lee, J.-H.; Song, J. Beamforming via array pattern synthesis for millimeter wave NOMA downlink transmission. *IEEE Trans. Veh. Technol.* **2018**, *67*, 12363–12367. [CrossRef]
20. Wang, W.; Teh, K.C.; Li, K.H. Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 505–515. [CrossRef]

21. Cumanan, K.; Ding, Z.; Xu, M.; Poor, H.V. Secrecy rate optimization for secure multicast communications. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1417–1432. [CrossRef]
22. Zheng, K.; Ou, S.; Yin, X. Massive MIMO channel models: A survey. *Int. J. Antennas Propag.* **2014**, *2014*, 848071. [CrossRef]
23. Muhi-Eldeen, Z.; Ivrissimtzis, L.; Al-Nuaimi, M. Modelling and measurements of millimeter wavelength propagation in urban environments. *IET Microw. Antennas Propag.* **2010**, *4*, 1300–1309. [CrossRef]
24. Luo, Z.; Ma, W.; So, A.; Ye, Y.; Zhang, S. Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Process. Mag.* **2010**, *27*, 20–34. [CrossRef]
25. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.
26. Havary-Nassab, V.; Shahbazpanahi, S.; Grami, A.; Luo, Z. Distributed beamforming for relay networks based on second-order statistics of the channel state information. *IEEE Trans. Signal Process.* **2008**, *56*, 4306–4316. [CrossRef]
27. Sturm, J.F. Using SeDuMi 1.02, a Matlab toolbox for optimization over symmetric cones. *Optim. Methods Softw.* **1999**, *11–12*, 625–653. [CrossRef]
28. Lofberg, J. YALMIP: A toolbox for modeling and optimization in MATLAB. In Proceedings of the CACSD Conference, Taipei, Taiwan, 2–4 September 2004.
29. Karipidis, E.; Sidiropoulos, N.D.; Luo, Z.-Q. Quality of service and max-min fair transmit beamforming to multiple cochannel multicast groups. *IEEE Trans. Signal Process.* **2008**, *56*, 1268–1279. [CrossRef]
30. Fuchs, B.; Skrivervik, A.; Mosig, J.R. Synthesis of uniform amplitude focused beam arrays. *IEEE Antennas Wirel. Propag. Lett.* **2012**, *11*, 1178–1181. [CrossRef]