Physical Layer Security of Space-Division Multiplexed Fiber-Optic Communication Systems in the Presence of Multiple Eavesdroppers

Kyle Guan, Peter J. Winzer, Antonia M. Tulino, and Emina Soljanin
Bell Labs, Alcatel-Lucent, Holmdel, NJ, USA

***Abstract*—In this paper, we examine the information-theoretic security of multiple-input-multiple-output space-division multiplexed (MIMO-SDM) fiber-optic communication systems in the presence of multiple eavesdroppers. In particular, we analyze the achievable secrecy rate for the two special cases that reflect different capabilities of the eavesdroppers: independent eavesdroppers who do not share received information and colluding (cooperating) eavesdroppers who can combine and jointly process the received signals. Our results show that MIMO-SDM systems are robust against multiple independent tapping attacks, in the sense that the average achievable secrecy rate is strictly positive even with an infinite number of eavesdroppers. Though extremely difficult to implement in practice, if all the eavesdroppers could cooperate coherently, the average secrecy rate decreases quickly with the number of eavesdroppers. As such, to counter the colluding eavesdroppers, a combination of much higher SNR for the legitimate receiver and higher mode-dependent loss (MDL) for the eavesdroppers is needed.**

I. Introduction

Recent developments in the field of space-division multiplexing (SDM) for fiber-optic communication systems suggest that SDM can not only increase system capacity, but can also achieve provable security against physical layer attacks, such as fiber tapping via evanescent coupling [1]-[12]. Compared to the case of a single mode fiber, tapping by coupling spatial signals out of an optical MIMO-SDM waveguide through bending leads to inherent changes in the spatial information content, for both eavesdropper and legitimate transmitter-receiver pair. As a result, the MIMO channel of the eavesdropper will be generally less favorably conditioned than that of the legitimate user; at the same time, a bend-induced mode-dependent loss (MDL) recorded at the legitimate receiver can reveal the possible presence of an eavesdropper. In our previous research [8]-[12], we evaluated the security benefits of MIMO-SDM *with a single eavesdropper* by using the information theoretic framework developed in [13]-[20]. Our results show that the secrecy capacity achieved by an optical MIMO-SDM system can be orders of magnitude higher than what can be offered by quantum techniques, e.g., quantum key distribution (QKD), albeit with a slightly different notion of security based on classical information theory as opposed to on quantum mechanical principles. In addition, SDM systems can provide fundamental security even if an eavesdropper has a higher SNR than the legitimate receiver [12].

In this paper, we expand our information-theoretic security analysis of SDM fiber-optic communication systems by looking into the scenarios that involve *multiple, potentially coherently cooperating* wire-tapping eavesdroppers, as conceptually illustrated in Fig. 1 (a). Such scenarios could arise both from localized multi-tapping as well as from multiple tapping locations that are distributed across a MIMO-SDM link spanning thousands of kilometers. Moreover, sophisticated eavesdroppers could potentially exchange and combine all the received signals coherently, thus enhancing their capability to jointly receive/decode the confidential information. As such, we focus on characterizing the secrecy capacity/achievable secrecy rate of MIMO-SDM systems in the presence of multiple eavesdroppers. In particular, we consider two cases that represent different levels of sophistication of the eavesdroppers: independent eavesdroppers who do not exchange tapped signals and colluding (cooperating) eavesdroppers who can combine and jointly process the received signals coherently. The results allow us to assess the impact of multiple eavesdroppers as well as the key system parameters on the information-theoretic security of MIMO-SDM systems.

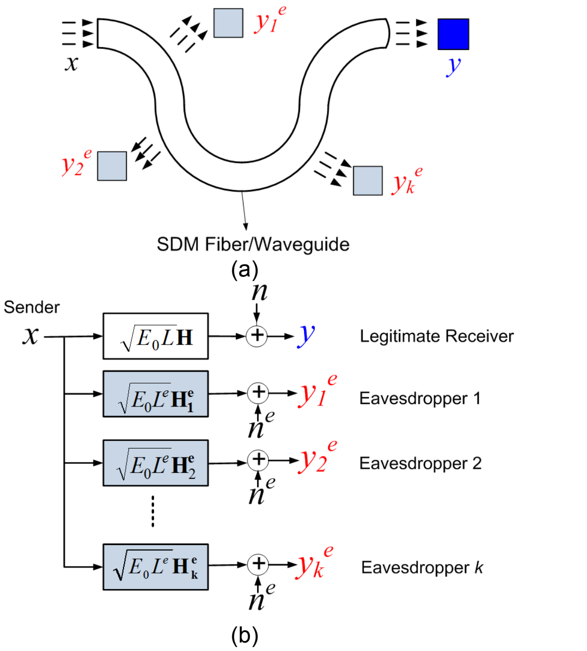

Fig. 1. (a) SDM waveguide transmission in the presence of multiple eavesdroppers; (b) the corresponding system model.

978-1-4799-5952-5/15/$31.00 ©2015 IEEE

A. Related Work

Various vulnerabilities and security issues of fiber-optic transmission systems are surveyed in [1]-[4], with [1] providing a detailed analysis of fiber tapping mechanisms. The fundamental results from the vast body of research [13]-[22] in information-theoretic security for wireless communications provide the theoretical foundations for our research. The concepts of equivocation and secrecy capacity were first introduced by Wyner [13]. In [14], Leung-Yan-Cheong and Hellman studied the single-input-single-output (SISO) Gaussian channel and showed that the secrecy capacity equals the difference between the capacities of main and eavesdropping channel. The secrecy capacity of wireless fading channels and free-space optical channels was characterized in [15] and [16], respectively. The results in [17]-[20] provide the theoretical foundations for analyzing the secrecy capacity of a MIMO wire-tap channel with channel state information (CSI) known at the transmitter and receiver. Our research is particularly informed by [21] and [22], which analyzed secrecy capacity and achievable secrecy rate for wireless systems in the presence of multiple eavesdroppers.

The rest of the paper is organized as follows. In Section II we provide a brief overview of fiber-optic MIMO-SDM systems and describe the system model for SDM waveguide tapping with multiple eavesdroppers. In Section III we summarize our previous results of the secrecy capacity for MIMO-SDM systems with a single eavesdropper. In Section IV we analyze the achievable secrecy rate of MIMO-SDM systems with multiple eavesdroppers. In particular, we consider two cases: independent eavesdroppers and colluding eavesdroppers. In Section V we discuss the implications of the key results and summarize our main findings.

II. SDM Waveguide and Fiber Tapping Model

A. Characteristics of Optical MIMO-SDM Systems

To be economically viable, SDM technologies leverage *integration* of system components among parallel spatial channels [5], [6]. Since integration often comes at the expense of *crosstalk* among parallel paths, MIMO techniques, originally developed for wireless systems, are used to mitigate crosstalk [23], [24]. Compared to MIMO wireless systems, fiber-optic MIMO-SDM systems have some unique characteristics [7]. For example, the receiver-to-transmitter feedback delays in optical transport systems are comparable with the time constants expected for MIMO-SDM channel dynamics. Thus there is no CSI at the transmitter. Also, the MIMO-SDM channel can be approximated as a "perturbed unitary" channel. Further, the transmit power is constrained for each mode individually due to fiber nonlinear effects, instead of having a total average power constraint that is normally used in the study of wireless MIMO systems. These characteristics are incorporated into the models and formulations used in our work.

B. System Model

Fig. 1 (a) illustrates the scenario of fiber-tapping with multiple eavesdroppers. A signal vector $\mathbf{x}$ is transmitted through an SDM waveguide and received by a legitimate receiver as $\mathbf{y}$. There are k eavesdroppers wire-tapping the waveguide. As such, signal $\mathbf{x}$ is also received by the ith eavesdropper as $\mathbf{y_i^e}$. The abstraction of the channel model is shown in Fig. 1 (b). Specifically, we consider the SDM system that supports a set of M orthogonal propagation modes, which are subject to coupling and MDL. Here we ignore the fiber inter- and intra-modal nonlinearities and model the SDM system as a linear matrix MIMO channel. That is, we use $M \times M$ (normalized) matrices $\mathbf{H}$ and $\mathbf{H_i^e}$ to represent the realizations of the legitimate and the ith eavesdropping channel, respectively. Assuming that the noise generated within the receiver dominates, the received signals $\mathbf{y}$ and $\mathbf{y_i^e}$ are

$$\mathbf{y} \;=\; \sqrt{E_0}\sqrt{L}\mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

$$\mathbf{y_i^e} \;=\; \sqrt{E_0}\sqrt{L_i^e}\mathbf{H_i^e}\mathbf{x} + \mathbf{n_i^e},\ i = 1, ..., k, \tag{2}$$

where L and L_i^e are normalization factors, with $L = \mathrm{tr}\{\tilde{\mathbf{H}}\tilde{\mathbf{H}}^\dagger\}/M$ and $L_i^e = \mathrm{tr}\{\tilde{\mathbf{H}}_\mathbf{i}^\mathbf{e}\tilde{\mathbf{H}}_\mathbf{i}{}^{\mathbf{e}\dagger}\}/M$. L and L_i^e characterize the mode-average loss of the respective channels $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{H}}_\mathbf{i}^\mathbf{e}$ [7]. The distributions of channel noises $\mathbf{n}$ and $\mathbf{n_i^e}$ are circularly symmetric complex Gaussian with per-mode power spectral density N_0 and N_{0i}^e for the legitimate receiver and the ith eavesdropper, respectively.

As mentioned above, we make the realistic assumption that CSI is not available at the transmitter. However, the individual realization of $\mathbf{H}$ is known to the legitimate receiver via training symbols. Similarly, the channel realization of $\mathbf{H_i^e}$ is unknown to the transmitter, but can be estimated by and is known to the ith eavesdropper. We consider a phenomenological channel model for the effect of fiber bending. Motivated by an eavesdropper's desire to couple as little light out of the SDM fiber as possible (to avoid being detected), we assume that the legitimate channel remains essentially unperturbed, apart from a unitary transform. That is, we model $\mathbf{H}$ as a random unitary matrix: $\mathbf{H} = \mathbf{U}$, with $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}$; while an eavesdropper sees an MDL channel, with significant MDL from bending induced evanescent coupling. Specifically, we model $\mathbf{H_i^e}$ as a concatenation of two operations – a rotation operation $\mathbf{U_i^e}$ followed by a scaling operation $\sqrt{\mathbf{V_i^e}}$. That is, $\mathbf{H_i^e} = \sqrt{\mathbf{V_i^e}}\mathbf{U_i^e}$, where $\mathbf{U_i^e}$ is a random unitary matrix and $\mathbf{V_i^e}$ is a random diagonal matrix. We refer to $\mathbf{V_i^e}$ as the MDL matrix, with diagonal elements v_{ij}, $j = 1, ..., M$. We specify the value of MDL as the ratio of maximum v_{ij} to minimum v_{ij} [10][12]. For $M > 2$, the MDL matrix is not uniquely defined by the MDL value. The diagonal MDL matrix elements, expressed in decibels as $10\log_{10}(v_{ij})$, are randomly drawn from a uniform distribution in $[\min\{10\log_{10}(v_{ij})\}, \max\{10\log_{10}(v_{ij})\}]$. The specified MDL value is expressed in decibels as $\mathrm{MDL_{dB}} = 10\log_{10}(\max\{v_{ij}\}/\min\{v_{ij}\})$. Moreover, the v_{ij}s are subject to the (linear) trace normalization $\sum_{j=1}^{M} v_{ij} = M$ for $i = 1, ..., k$. We note that the MDL value is similar to the *condition number* of a channel matrix often used in the wireless MIMO literature [25]. An MDL value close to 0 dB means that the MIMO-SDM channel is well-conditioned; while a large MDL value indicates that the MIMO-SDM channel is illconditioned.

III. Secrecy Capacity with One Eavesdropper

To keep this paper self-contained, we summarize the most important results on the secrecy capacity of MIMO-SDM systems with a single eavesdropper, to provide a baseline for characterizing achievable secrecy rate of MIMO-SDM systems with multiple eavesdroppers.

A. Secrecy Capacity Per Channel Realization

As shown in [10][12], for given channel realizations $\mathbf{H} = \mathbf{U}$ and $\mathbf{H^e} = \sqrt{\mathbf{V^e}}\mathbf{U^e}$[1], the secrecy capacity of the optical MIMO-SDM channel is achieved by a circularly symmetric complex Gaussian input, with zero-mean and diagonal covariance $\mathbf{\Lambda_x}$, such that $\mathbb{E}[|x_j|^2] = \overline{P_j} \leq \overline{P}$. The secrecy capacity is given by

$$\begin{aligned} C_s = & \max_{\mathbf{\Lambda_x}} \log_2 \left[\det(\mathbf{I} + \mathrm{SNR}\mathbf{U}\mathbf{\Lambda_x}\mathbf{U}^\dagger)\right] \\ & - \log_2 \left[\det(\mathbf{I} + \mathrm{SNR}^e\sqrt{\mathbf{V^e}}\mathbf{U^e}\mathbf{\Lambda_x}\mathbf{U^{e\dagger}}\sqrt{\mathbf{V^e}})\right] \qquad (3) \\ & \text{s.t.}: \;\; \mathbb{E}[|x_j|^2] = \overline{P_j} \leq \overline{P}, \;\; j \in 1, ..., M. \end{aligned}$$

where $\mathrm{SNR} = LE_0/N_0$ and $\mathrm{SNR}^e = L^e E_0/N_0^e$ are the mode-averaged signal-to-noise ratios of the legitimate and eavesdropping channels, respectively; det denotes the determinant of a matrix. We emphasize that the power in optical SDM systems is constrained by fiber nonlinearities on a *per mode* basis. As such we set an upper bound $\overline{P_j} = \overline{P}$ for the power of each mode individually.

B. Average Secrecy Capacity

As mentioned in the previous section, the random channel realizations $\mathbf{H} = \mathbf{U}$ and $\mathbf{H^e} = \sqrt{\mathbf{V^e}}\mathbf{U^e}$ are unknown at the transmitter. Thus, the secrecy capacity of the MIMO-SDM channel is inherently a random quantity. Therefore, a meaningful characterization relies either on average or on outage values [10][12]. In this paper, we consider the cases where the signal experiences a large number of statistically independent channel realizations in frequency (e.g., optical MIMO-SDM systems with differential group delays significantly exceeding a symbol period). Consequently, we can average C_s over many channel realizations and a secrecy capacity of $C_s^{avg} = \langle C_s \rangle$ can be achieved. We refer to this capacity as *average secrecy capacity*. In [10][12], we show that the equal power allocation, i.e., $\mathbf{Q_x} = \overline{P}\mathbf{I}$ achieves the average secrecy capacity. That is, $\mathbf{H} = \mathbf{U}$ and $\mathbf{H^e} = \sqrt{\mathbf{V^e}}\mathbf{U^e}$, transmitting uncorrelated signals of equal power $\overline{P}$ on all modes will achieve the average secrecy capacity, which is given by

$$C_s^{avg} = \mathbb{E}[\sum_{i=1}^{M}[\log_2(1 + \mathrm{SNR}) - \log_2(1 + \mathrm{SNR}^e v_i)]]. \qquad (4)$$

IV. Secrecy Capacity with Multiple Eavesdroppers

In this section, we characterize the achievable secrecy rate of MIMO-SDM systems in the presence of multiple eavesdroppers. In particular, we consider two cases: independent eavesdroppers and colluding eavesdroppers.

A. The Case of Independent Eavesdroppers

For the case where all the eavesdroppers are mutually independent, we use the framework of general *compound wiretap channels* introduced in [21]. For given channel realizations $\mathbf{H}$ and $\mathbf{H_i^e}$, by directly applying Lemma 1 in [21] and incorporating the per mode power constraint, we can show that an achievable secrecy rate[2] per channel realization is given by

$$\begin{aligned} R_s = & \max_{\mathbf{\Lambda_x}} \min_{i \in 1,\ldots,k} \log_2 \left[\det(\mathbf{I} + \mathrm{SNR}\mathbf{U}\mathbf{\Lambda_x}\mathbf{U}^\dagger)\right] \\ & - \log_2 \left[\det(\mathbf{I} + \mathrm{SNR}^e\sqrt{\mathbf{V_i^e}}\mathbf{U_i^e}\mathbf{\Lambda_x}\mathbf{U_i^{e\dagger}}\sqrt{\mathbf{V_i^e}})\right] \qquad (5) \\ & \text{s.t.}: \;\; \mathbb{E}[|x_j|^2] = \overline{P_j} \leq \overline{P}, \;\; j \in 1, \; ..., \; M. \end{aligned}$$

With equal power allocation of $\overline{P_j} = \overline{P}$ on each mode, Eq. (5) can be simplified to

$$\begin{aligned} R_s \;\; = & \;\; \sum_{j=1}^{M} \log_2(1 + \mathrm{SNR}) \qquad (6) \\ - & \;\; \max_{i \in 1,\ldots,k} [\sum_{j=1}^{M} \log_2(1 + \mathrm{SNR}^e v_{ij})]. \end{aligned}$$

That is, to obtain the achievable secrecy rate, we first calculate the capacity for each of the k transmitter-eavesdropper pairs and select the pair with the largest capacity. The capacity difference between the transmitter-legitimate receiver pair and this particular transmitter-eavesdropper pair (with the largest capacity) is the achievable secrecy rate.

To understand how R_s changes with k, the number of eavesdroppers, we first run a simulation that generates 10^5 random channel realizations of $\mathbf{H} = \mathbf{U}$ and $k \times 10^5$ realizations of $\mathbf{H_i^e} = \mathbf{U_i^e}\sqrt{\mathbf{V_i^e}}$, for a given set of parameters M, k, MDL, SNR and SNR^e. For each channel realization, we calculate the corresponding R_s by using (6). In Fig. 2, we plot the distributions of R_s (normalized to $C_0 = \log_2(1 + \mathrm{SNR})$) for different k. In particular, we consider $k = \{1, 4, 16, 64, 128, 512\}$, $M = 8$, $\mathrm{SNR} = \mathrm{SNR}^e = 20$ dB, and[3] MDL = 20 dB. As shown in the plot, the distribution of R_s shifts towards lower secrecy rates with increasing k. In addition, the variance of R_s decreases as k increases. We also note that all the minimal R_s for each k are very close to each other, as shown in the inset in Fig. 2, in which the distribution of R_s is plotted on a logarithmic scale. In fact, independent of the number of eavesdroppers k, the distribution of secrecy rate is lower

[1] Since there is only one eavesdropper, we drop the index i associated with $\mathbf{V^e}$ and $\mathbf{U^e}$ in this section.

[2] Except for the simple case of $M = 2$, $\mathbf{H} = \mathbf{U}$ and $\mathbf{H_i^e} = \sqrt{\mathbf{V_i^e}}\mathbf{U_i^e}$ do not necessarily constitute *degraded* MIMO compound wiretap channels, as defined in [21]. Thus we can not directly apply the *secrecy capacity* result of Theorem 5 in [21].

[3] For simplicity, we assume that all the eavesdroppers have the same SNR^e and MDL values in this paper.

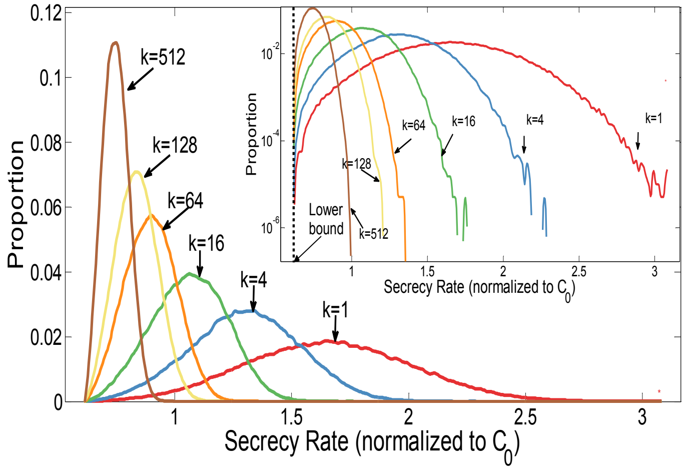

Fig. 2. The distributions of secrecy rate R_s for different numbers of non-cooperating eavesdroppers $k = \{1, 4, 16, 64, 128, 512\}$, with $M = 8$ modes, SNR = SNR^e = 20 dB, and a mode-dependent loss of MDL=20 dB.

bounded by the same value. The value of this lower bound equals the *guaranteed secrecy capacity* of the MIMO-SDM wiretap channel with a single eavesdropper [12]. The lower bound, denoted as R_s^{LB}, is given by

$$R_s^{LB} = MC_0 - C_e^{\max}, \tag{7}$$

where $C_e^{\max}$ can be obtained by solving the following optimization problem [12]:

$$\begin{aligned} \max_{v_i}: \quad & C_e = \sum_{i=1}^{M} \log_2(1 + \text{SNR}^e v_i) \\ \text{s.t.}: \quad & \sum_{i=1}^{M} v_i = M, \\ & v_2 = \text{MDL} v_1, \\ & v_1 \le v_i \le v_2, \quad i = 3, 4, ..., M. \end{aligned} \tag{8}$$

We note that R_s^{LB}, independent of k, depends only on M, MDL, SNR, and SNR^e.

The average secrecy rate is given by $R_s^{avg} = \mathbb{E}[R_s]$. To understand how different system parameters affect the average secrecy rate, in Fig. 3 we plot R_s^{avg} as a function of the number of eavesdropper k, for different MDL values. The plot shows that for a given k, the average secrecy rate is higher for an MIMO-SDM wiretap channel with larger MDL. We also note that though R_s^{avg} decreases monotonically with increasing k, the rate of decrease is fairly small. For example, for the case of MDL = 20 dB, it takes from 1 to about 128 eavesdroppers to reduce the average secrecy rate by half. As k further increases, the average secrecy rate plateaus. In the extreme case that $k \to \infty$, the average secrecy rate converges to the lower bound R_s^{LB}, as illustrated by the two dashed horizontal lines representing R_s^{LB}s for MDL = 5 dB and MDL = 10 dB, respectively. In other words, for MDL > 0 dB, the average secrecy rate is strictly positive even in the presence of infinite many eavesdroppers, as long as these eavesdroppers act independently and do not exchange received signals and information.

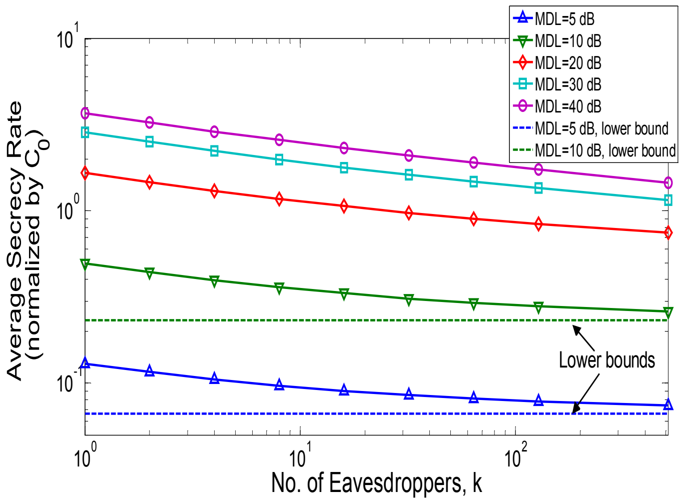

Fig. 3. The average secrecy rate R_s^{avg} as a function of the number of non-cooperating eavesdropper k, for different values of mode-dependent loss (MDL), with $M = 8$ modes, and SNR = SNR^e = 20 dB.

B. The Case of Colluding Eavesdroppers

In this section, we consider the case where all eavesdroppers have the capability to cooperate. In particular, we assume that the eavesdroppers are capable of measuring and exchanging the full optical field across all modes, which would require enormous complexity in practice. We follow the approach used in [22], where the authors studied the single-input-single-output (SISO) Gaussian wiretap channel with multiple colluding eavesdroppers. In particular, we consider the worst case scenario that each eavesdropper sends the received signals to a centralized unit for coherent combining /processing, which also requires tremendous complexity in the context of optical MIMO-SDM transmission [26]. The centralized processing allow eavesdroppers to benefit from the redundant observations and thus produce a better estimate of the secret message in comparison to each of the individual estimates.

In [22], the functionality of a central unit to process the collection of signals received by all eavesdroppers is modeled as a single-input-multiple-output (SIMO) channel. Informed by this approach, we model the collections of received signal $\mathbf{y_i^e}$s as $\mathbf{y^e} = [\mathbf{y_1^e}, \mathbf{y_2^e}, ..., \mathbf{y_k^e}]^T$. That is, we combine all the received y_i^es as a single $kM \times 1$ column vector, as shown in Fig. 4. Similarly, k of $M \times M$ eavesdropping channels are combined into a single $kM \times M$ wiretap channel, which is given by

$$\begin{aligned} \mathbf{H^e} &= [\mathbf{H_1^e}, \mathbf{H_2^e}, ..., \mathbf{H_k^e}]^T \\ &= [\sqrt{\mathbf{V_1^e}}\mathbf{U_1^e}, \sqrt{\mathbf{V_2^e}}\mathbf{U_2^e}, ..., \sqrt{\mathbf{V_k^e}}\mathbf{U_k^e}]^T \end{aligned} \tag{9}$$

In other words, k cooperating eavesdroppers are equivalent to one "super" eavesdropper, whose received signal and wiretap channel are characterized by $\mathbf{y}$ and $\mathbf{H^e}$, respectively. By

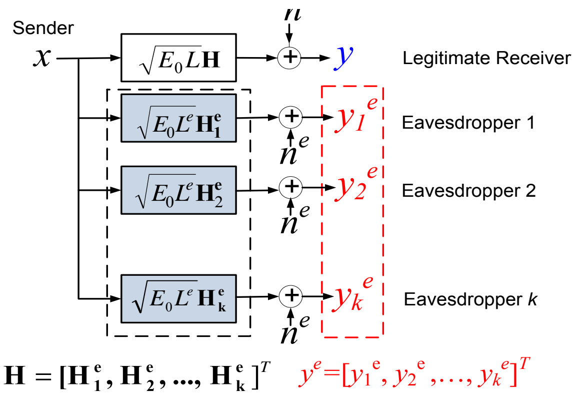
Sender
x
$\sqrt{E_0 L}\mathbf{H}$
n
y
Legitimate Receiver
$\sqrt{E_0 L^e}\mathbf{H}_1^e$
n^e
y_1^e
Eavesdropper 1
$\sqrt{E_0 L^e}\mathbf{H}_2^e$
n^e
y_2^e
Eavesdropper 2
$\sqrt{E_0 L^e}\mathbf{H}_k^e$
n^e
y_k^e
Eavesdropper k
$\mathbf{H} = [\mathbf{H}_1^e, \mathbf{H}_2^e, ..., \mathbf{H}_k^e]^T$
$y^e=[y_1^e, y_2^e, \dots, y_k^e]^T$

Fig. 4. System model for colluding eavesdroppers.

treating the colluding eavesdroppers as one eavesdropper, we can apply our previous results on the average secrecy capacity (for a single eavesdropper). Assuming equal power allocation of $\overline{P}$ on all the modes, the average achievable secrecy rate[4] is

$$R_s^{avg} \quad = \quad \mathbb{E}\{R_s\}, \qquad (10)$$

where R_s is given by

$$\begin{aligned} R_s \quad &= \quad \max\{\log_2\left[\det(\mathbf{I}+\text{SNR}\mathbf{H}\mathbf{H}^\dagger)\right] \qquad (11)\\ &- \quad \log_2\left[\det(\mathbf{I}+\text{SNR}^e\mathbf{H^e}\mathbf{Q_x}\mathbf{H^e}^\dagger)\right], 0\}\\ &= \quad \max\{\log_2 MC_0\\ &- \quad \log_2\left[\det(\mathbf{I}+\text{SNR}^e\mathbf{H^e}\mathbf{H^e}^\dagger)\right], 0\}\\ &= \quad \max\{\log_2 MC_0\\ &- \quad \sum_{j=1}^{kM}\log_2(1+\lambda_j^e\text{SNR}^e), 0\}. \end{aligned}$$

Here, λ_j^es are eigenvalues of $\mathbf{H^e}\mathbf{H^e}^\dagger$. We note that by definition the secrecy rate is a non-negative quantity. Thus R_s is zero if $\log_2 MC_0 - \sum_{j=1}^{kM}\log_2(1+\lambda_j^e\text{SNR}^e) < 0$. Eq. (11) shows that the "super" eavesdropper has a power gain by combing all the received signals from the eavesdroppers. That is, the capacity of the main channel is proportional to M; while the capacity of the combined eavesdropping channel is proportional to kM (there are kM summation terms in $\sum_{j=1}^{kM}\log_2(1+\lambda_j^e\text{SNR}^e)$). Depending on the values of M, k, λ_j^e, SNR, and SNR^e, this power gain could have a detrimental effect on the security of the transmitter- legitimate receiver pair, in the sense that R_s could quickly decrease to zero as the number of eavesdroppers increases. Fig. 5 (a) illustrates such a case. We plot the distributions of R_s for $k = \{1,\ 2\}$, with $M = 8$, SNR=20 dB, SNR^e=18 dB, and MDL=20 dB. Even with two eavesdroppers, there is a considerable number of channel instantiations that results in zero secrecy rate, as indicated by the distribution of R_s for $k = 2$. To enhance the security against multiple cooperating eavesdroppers, the legitimate receiver must have much higher SNR than the eavesdroppers have, as shown in Fig. 5 (b), which plots the distributions of R_s for $k = \{1, 2, 4, 8, 10\}$, with $M = 8$, SNR=20 dB, SNR^e=10 dB, and MDL=20 dB. When the SNR of the legitimate receiver is 10 dB higher than that of the eavesdroppers, the system can have a strictly positive average secrecy rate for up to 10 coherently cooperating eavesdroppers.

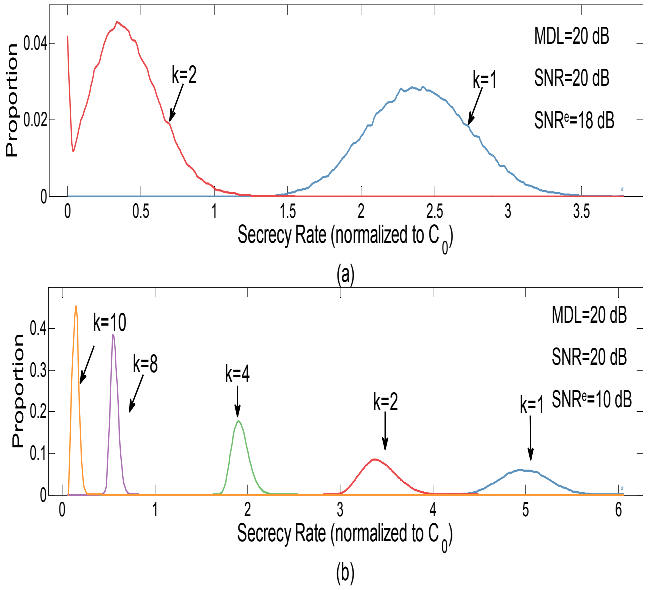

Fig. 5. (a) Distributions of secrecy rate R_s for $k = \{1,\ 2\}$, with $M = 8$ modes, SNR=20 dB, SNR^e=18 dB, and a mode-dependent loss of MDL=20 dB; (b) distributions of secrecy rate R_s for $k = \{1, 2, 4, 8, 10\}$, with $M = 8$ modes, SNR=20 dB, SNR^e=10 dB, and a mode-dependent loss of MDL=20 dB.

To evaluate how different system parameters affect the average secrecy rate in the presence of colluding eavesdroppers, we plot in Fig. 6 the average secrecy rate R_s^{avg} as a function of the number of eavesdroppers k, for different MDL and SNR^{e}values. These curves indicate that the average secrecy rate decreases rapidly with an increasing number of colluding eavesdroppers. When k increases beyond a certain threshold, the average secrecy rate approaches zero. To enhance the robustness of a MIMO-SDM system against a large number of cooperating eavesdroppers, a higher SNR for the legitimate receiver, a larger MDL for the eavesdroppers, or a combination of both is needed.

V. Discussions and Conclusions

In this work, we have evaluated the achievable secrecy rate of MIMO-SDM systems in the presence of multiple eavesdroppers. In particular, we consider two cases: independent eavesdroppers who do not exchange tapped signals and colluding eavesdroppers who can coherently combine and jointly process the received signals. Our results show that MIMO-SDM systems are fairly robust against multiple independent tapping attacks, in the sense that the average secrecy rate is strictly positive even in the presence of infinite many

[4] We are still investigating whether equal power allocation is capacity achieving for $\mathbf{H^e}$ as given in Eq. (9).

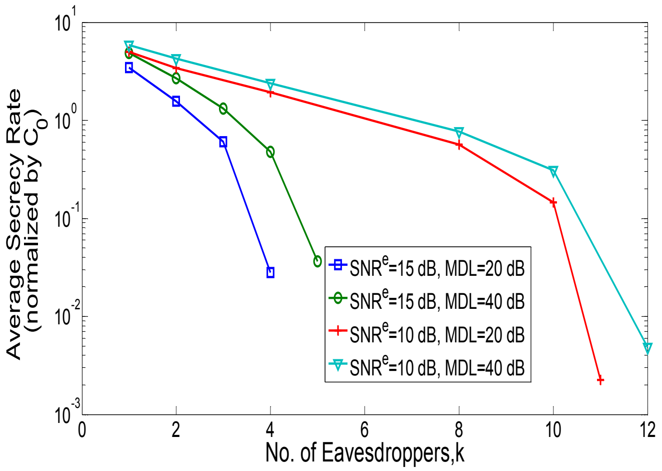

Fig. 6. The average secrecy rate R_s^{avg} as a function of the number of cooperating eavesdropper k, for different MDL and SNR^{e}values, with $M = 8$ modes and SNR $= 20$ dB.

non-cooperating eavesdroppers. However, if the eavesdroppers have the capability to coherently combine and then process their received information, which requires tremendous complexity to implement in practice, the average secrecy rate could decrease quickly. As such, defending MIMO-SDM systems against colluding eavesdroppers often requires a combination of much higher SNR for the legitimate receiver and higher MDL value for the eavesdroppers.

References

[1] K. Shaneman and S. Gray, “Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention,” in *Military Communications Conference*, Monterey, CA, 2004, vol. 2, pp.711-716.

[2] M. Medard, *et al.*, “Security issues in all-optical networks,” *IEEE Netw.*, vol. 11, no. 3, pp. 42-48, May/June, 1997.

[3] M. P. Fok, Z. Wang, Y. Deng, and P. R. Pucnal, “Optical layer security in fiber-optic networks,” *IEEE Transactions on Information Security and Forensics*, vol., no. , pp. 725-736, Sept. 2011.

[4] B. Wu, B. J. Shasti, P. R. Prucnal, “Secure communication in fiber-optic networks,” *Emerging Trends in ICT Security*, Elsevier, 2014.

[5] P. J. Winzer, “Spatial multiplexing: the next frontier in network capacity scaling,” in *Proc. Eur. Conf. Optical Communication*, 2013, Paper We.1.D.1.

[6] P. J. Winzer, “Making spatial multiplexing a reality,” *Nature Photonics*, vol. 8, pp. 345-348, 2014.

[7] P. J. Winzer and G. J. Foschini, “MIMO capacities and outage probabilities in spatially multiplexed optical transport systems,” *Optical Express*, vol. 19, no. 17, pp. 16680-16696, Aug. 2011.

[8] K. Guan, P. J. Winzer, and E. Soljanin, “Information-theoretic security in space-division multiplexed fiber optic networks,” *38th European Conference and Exhibition on Optical Communication (ECOC 2012)*, Tu.3.C.4, Amsterdam, Netherlands, Sep. 2012.

[9] K. Guan, E. C. Song, E. Soljanin, P. J. Winzer, and Tulino, A. M, “Physical layer security in space-division multiplexed fiber optic communications,” In IEEE Signals, Systems and Computers (ASILOMAR), 2012 Conference of the Forty Sixth Asilomar Conference on, pp. 654-658, Asilomar, CA, Nov. 2012.

[10] K. Guan, P. J. Winzer, E. Soljanin, and A. M. Tulino, “On the secrecy capacity of the space-division multiplexed fiber optical communication system, ” in *IEEE Conference on Communication and Network Security (CNS)*, Washington D.C., 2013, pp.207-214.

[11] E. C. Song, E. Soljanin, P. Cuff, H. V. Poor, and K. Guan, “ Rate-distortion-based physical layer secrecy with applications to multimode fiber,”*IEEE Transactions on Communications*, vol. 62, no. 3, pp. 1080-1090, Mar. 2014.

[12] K. Guan, A. M. Tulino, P. J. Winzer, and E. Soljanin, “Secrecy capacities in space-division multiplexed fiber optic communication systems,” *IEEE Trans. Inf. Forensics Security* , accepted and to be published in 2015.

[13] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp.1355-1387, Oct. 1975 .

[14] S. K. Cheong and M. Hellman,“The Gaussian wire-tap channel”, *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp.451-456, Jul. 1978.

[15] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” *ISIT* 2006, Seattle, WA, USA, Jul. 2006.

[16] F. J. Lopez-Martinex, G. Gomez, J. M. Garrido-Balsells, “Physical-layer security in free-space optical communications,” *IEEE Photonics Journal*, vol. 7, no. 2, pp. 1-15, Apr. 2015.

[17] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” IEEE Trans. Inf Theory, vol. 57, no. 8, pp. 4961-4971, Aug. 2011.

[18] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas-I: the MISOME wiretap channel, ” *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.

[19] A. Khisti and G. W. Wornell, “Secure Transmission with multiple antennas-II: the MIMOME wiretap channel,” *IEEE. Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.

[20] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), “An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel,” *EURASIP J. Wireless Commun. Network.*, pp. 2602-2606, 2009.

[21] Y. Liang, G. Karamer, H. V. Poor, and S. Shamai (Shitz), “Compound wiretap channels,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 5:15:12, March 2009.

[22] P. C. Pinto, J. Barros, and M. Z. Win, “Wireless physical-layer security: the case of colluding eavesdroppers,” *ISIT* 2009, Seoul, Korea, June 28-July 3, 2009.

[23] R. Ryf, *et al.*, “Mode-Division Multiplexing Over 96 km of Few-Mode Fiber Using Coherent 6 × 6 MIMO Processing,” in *IEEE/OSA JJ. Lightw. Technol.*, vol. 30, no. 4, pp. 521-531, Feb. 2012.

[24] S. Randel, *et al.*, “Adaptive MIMO signal processing for mode-division multiplexing,” in *Proc. Opt. Fiber Commun. Conf.*, 2012, Paper PDP5C.5.

[25] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, 2005.

[26] S. Randel, *et al.*,“Complexity analysis of adaptive frequency-domain equalization for MIMO-SDM transmission,” in *39th European Conference and Exhibition on Optical Communication (ECOC 2013)*, pp. 801-803.