Physical Layer Security in Space-Division Multiplexed Fiber Optic Communications

Kyle Guan*, Eva C. Song*†, Emina Soljanin*, Peter J. Winzer*, and Antonia M. Tulino*
*Bell Labs, Alcatel-Lucent, Holmdel, NJ, USA
†EE Department, Princeton University, Princeton, NJ USA

***Abstract*—Recent developments in the field of space-division multiplexing (SDM) for fiber-optic communication systems suggest that the spatial diversity offered by SDM can be used not only to increase system capacity, but also to achieve provable security against physical layer attacks. In this work, we outline some of the mathematical framework necessary to assess the security benefits of the SDM. We substantiate our conjecture that allocating the maximal allowable power to each mode is optimal in terms of physical layer security. Further more, we expand the scope of our security analyses to include distortion as a quantitative metric for secrecy and study how the rate of reliable communication between the legitimate transmitter-receiver pair can be chosen to maximize reconstruction (decoding) errors of the eavesdropper.**

I. Introduction

Fiber-optic communication systems are inherently vulnerable to various types of physical-level attacks [1]. The most common form of attack is fiber tapping, where an attacker with physical access to the fiber retrieves a portion of the propagating signals by bending the fiber and detecting the evanescent field at the bend. Moreover, by introducing a sufficiently small amount of bending loss (e.g., by tapping at a point of high optical signal power near an optical amplifier), a fiber-tapping eavesdropper can go unnoticed by the legitimate transmitter and receiver. The wide availability of fiber tapping devices and the difficulty of detecting wire-tapping are physical-layer security concerns. Quantum key distribution (QKD) addresses both concerns via the exchange of a secure key between a transmitter and a receiver while at the same time providing for intrusion detection [2], both provably secure based on fundamental quantum mechanical principles. However, the provable secure benefits of QKD come with stringent limitations in terms of both the secure data rate and the transmission reach (e.g., 1 Mb/s over 100 km of fiber [3]). Moreover, severe problems arise from optical amplifier noise and from interactions between classical communications and QKD signals on a common optical networking infrastructure [4].

Given that space-division multiplexing (SDM) has recently been shown to sustainably overcome the nonlinear Shannon limit of optical fiber [5]-[10], physical-layer security considerations of SDM have become important as well [11]. In fact, it has been shown that independent of the capacity scaling, SDM has the potential to ensure the physical-layer confidentiality of information transmission [11]. Coupling spatial information out of an SDM waveguide changes the spatial information content both for the eavesdropper and for the legitimate transmit-receiver pair. As a result, the eavesdropper's channel will generally be 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 will inherently reveal the presence of the eavesdropper. Expanding upon initial quantitative security results presented in [11], we present some mathematical foundations for evaluating the potential benefit of SDM in providing an information-theoretically provably secure way for information transmission in this paper. We first use equivocation (conditional entropy) as a metric of secrecy and provide a more detailed analysis of secrecy capacity for MIMO-SDM systems. In particular, we study the optimal power allocation strategy under the realistic assumption that legitimate receiver and eavesdropper know only their respective channel realization and that receiver-to-transmitter feedback is not possible. Based on both analytical and numerical results, we provide justification to our claim that allocating maximal allowable power to each mode is indeed optimal. In addition to equivocation, we also use distortion as the quantitative measure of secrecy to study how the possible rate of reliable communication between the legitimate transmitter-receiver pair can be chosen to incur maximal reconstruction (decoding) errors for the eavesdropper.

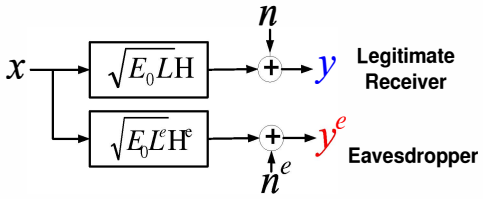

Fig. 1. System model: received signal by the legitimate receiver y and the eavesdropper y^e.

The rest of the paper is organized as follows. In Section II, we provide the MIMO-SDM waveguide and fiber tapping model. In Section III, we formulate the secrecy capacity problem for the MIMO-SDM systems. We also study the optimal power allocation strategies. In Section IV, we introduce distortion as a measure for secrecy and analyze the trade-off between transmission rate and distortion. We conclude the paper in Section V.

II. SDM Waveguide and Fiber Tapping Model

The SDM waveguide and fiber tapping models are shown in Fig. 1. The SDM waveguide supports a set of M orthogonal propagation modes that may be subject to coupling and differential gain or loss. Similar to the approach in [7], we ignore inter- and intra-modal fiber nonlinearities and model the SDM system as a linear matrix MIMO channel. In particular, the received signals of the legitimate receiver y and the eavesdropper y^e are:

$$y = \sqrt{E_0}\sqrt{L}\mathbf{H}x + n, \quad (1)$$

$$y^e = \sqrt{E_0}\sqrt{L^e}\mathbf{H^e}x + n^e, \quad (2)$$

where $\mathbf{H}$ and $\mathbf{H^e}$ are $M \times M$ (normalized) matrices for the legitimate and eavesdropping channels; L and L^e represent normalization factors with $L = \text{tr}\{\tilde{\mathbf{H}}\tilde{\mathbf{H}}^\dagger\}/M$ and $L^e = \text{tr}\{\tilde{\mathbf{H}}^\mathbf{e}\tilde{\mathbf{H}}^{\mathbf{e}\dagger}\}/M$ reflecting the mode-average loss of the respective channels $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{H}}^\mathbf{e}$ [7]. We model the channel noise n and n^e as symmetric complex Gaussian with per-mode power spectral density N_0 and N_0^e for the legitimate and eavesdropping receiver, respectively. In our model, we assume an uninformed transmitter. That is, the individual realization of $\mathbf{H}$ is known only to the legitimate receiver (e.g, through the use of training symbols) and unknown to the transmitter due to the long round trip delay in optical transmission systems. Similarly, the instances of $\mathbf{H^e}$ are known only to the eavesdropper and unknown to the transmitter.

Since realistic spatially resolved models for evanescent coupling of SDM fibers at a bend are not yet available, we assume a phenomenological model: legitimate channel remains essentially unperturbed, which is motivated by the eavesdroppers desire to coupe as little light out of the SDM fiber as possible in order to avoid being detected. The eavesdropper sees a mode-dependent loss (MDL) channel after evanescent coupling. While we show that the statistics of the MDL quantitatively affects the secrecy capacity, we believe that the exact nature of the channel model is not expected to qualitatively affect our results. Mathematically, we model $\mathbf{H}$ as a random unitary matrix.

For $\mathbf{H}^e$, we provide three different models as follows.

- Uniform distributed MDL model: $\mathbf{H^e} = \mathbf{U^e}\sqrt{\mathbf{V^e}}$, where $\mathbf{U^e}$ is a random unitary matrix and $\sqrt{\mathbf{V^e}}$ is a diagonal matrix. The diagonal elements $\sqrt{v_{ii}^e}$, which are on a linear scale and satisfy $\sum_{i=1}^{M} v_{ii}^e = M$, are randomly drawn from a uniform distribution: $[\min\{v_{ii}^e\}, \max\{v_{ii}^e\}]$. The mode-dependent loss, expressed in dB, is defined as $10^{\text{MDL}/10} = \max\{v_{ii}^e\}/\min\{v_{ii}^e\}$.
- Log-uniform distributed MDL model: $\mathbf{H^e} = \mathbf{U^e}\sqrt{\mathbf{V^e}}$. Here, the diagonal elements of $\sqrt{\mathbf{V^e}}$, now expressed in dB, are randomly drawn from a uniform distribution $[\min\{v_{ii}^e\}, \max\{v_{ii}^e\}]$. The diagonal elements are $10^{v_{ii}^e/20}$, with $\sum_{i=1}^{M} 10^{v_{ii}^e/10} = M$. The mode-dependent loss is then defined as MDL $= \max\{v_{ii}^e\} - \min\{v_{ii}^e\}$.
- Partial mode extraction model: we assume that the eavesdropper can perfectly extract only M_{rx} (out of M) modes, while experiencing significant MDL on the remaining $M - M_{rx}$ modes [7]. In particular, we model $\mathbf{H}^e$ as an $M \times M$ diagonal and *deterministic* matrix. Among the M diagonal elements, M_{rx} elements are of unit value and the remaining $M - M_{rx}$ ones are of value of $(10^{-MDL/20})$.

III. Secrecy Capacity of the MIMO-SDM Systems

A. Secrecy capacity

We first study the information-theoretic security of the SDM system, since this is widely accepted as the strictest notion of security. An important performance metric that characterizes the system is the *secrecy capacity*, which quantifies the maximum amount of information that can be transmitted from a legitimate transmitter to a legitimate receiver such that a wiretapping eavesdropper cannot receive any useful information [12]-[14]. Mathematically, this means that the equivocation (randomness) of the source, measured by the information entropy, is not reduced for the eavesdropper when observing the outputs from the wiretap channel. For given channel realizations of $\mathbf{H}$ and $\mathbf{H}^e$, we use the well-established formalism to derive the secrecy capacity C_s of a MIMO-SDM channel [14], with a modification of the assumptions that reflect the physical characteristics of an optical MIMO-SDM systems:

$$\begin{aligned} C_s &= \max_{\mathbf{Q_x}}[I(x,y) - I(x,y^e)] \\ &= \max_{\mathbf{Q_x}}[\log_2 \det(\mathbf{I} + \text{SNR}\mathbf{H}\mathbf{Q_x}\mathbf{H}^\dagger) \\ &\quad - \log_2 \det(\mathbf{I} + \text{SNR}^e\mathbf{H^e}\mathbf{Q_x}\mathbf{H^{e\dagger}})] \\ &\quad \text{subject to } E[x_i^2] < P_0. \end{aligned} \quad (3)$$

Here $I(x,y)$ and $I(x,y^e)$ denote the mutual information between the transmitter and the legitimate receiver and the mutual information between the transmitter and the eavesdropper, respectively. In addition, det and $\mathbf{Q_x}$ are the determinant of the matrix and the covariance matrix of the transmitted signal x, respectively. Note that we constrain the maximum optical power P_0 on a per-mode basis (as opposed to the total average power [14]) following the fiber nonlinearity arguments in [7].

In regard to the optimal $\mathbf{Q_x}$ that maximizes $I(x,y) - I(x,y^e)$, we conjecture that $\mathbf{Q_x} = P_0 I$. That is, sending uncorrelated signals of equal power of P_0 on all the modes is the optimum power allocation strategy under our assumption of an uninformed transmitter. We will detail the substantiation of our conjecture in Section III.C. With $\mathbf{Q_x} = P_0 I$, the expression of the C_s can be simplified as:

$$C_s = \sum_{i=1}^{M}[\log_2(1 + \text{SNR}\lambda_i) - \log_2(1 + \text{SNR}^e\lambda_i^e)], \quad (4)$$

where λ_i and λ_i^e are the non-zero eigenvalues of $\mathbf{H}\mathbf{H}^\dagger$ and $\mathbf{H^e}\mathbf{H^{e\dagger}}$, respectively, and SNR $= LE_0/N_0$ and SNR^e $= L^eE_0/N_0^e$ are the mode-averaged signal-to-noise ratios of the legitimate and wiretap channels. The capacity per mode of the legitimate channel C_0 is given by $C_0 = \log_2[1 + \text{SNR}]$, due to our unitary assumption of $\mathbf{H}$. We further normalize C_s by

MC_0 and arrive at

$$\frac{C_s}{MC_0} = 1 - \frac{\sum_{i=1}^{M} \log_2\left[(1+\text{SNR}^e\lambda_i^e)\right]}{MC_0}. \quad (5)$$

This is the maximum rate, in the unit of the raw SDM channel capacity, that can be transmitted in perfect information-theoretic secrecy over a particular MIMO-SDM channel instantiation (characterized by SNR^e and λ_i^e). We also note that if the capacity of the eavesdropper's channel is larger than that of the legitimate receiver ($\sum_{i=1}^{M} \log_2\left[(1+\text{SNR}^e\lambda_i^e)\right] > MC_0$), we set the secrecy capacity C_s/MC_0 to zero.

B. Probability of interception and outage secrecy capacity

For both uniformly and log-uniformly distributed MDL models, we assume that due to random mode coupling within the SDM fiber we cannot predict which of the transmit signals will be extracted stronger than others by the eavesdropper. As such, there exists a finite (low) probability that the instantaneous secrecy capacity C_s is exceedingly small. This is illustrated in Fig. 2(a), which shows a statistical distribution of the secrecy capacity C_s based on 10^5 random channel realizations for the case of $M = 8$, SNR=SNR^e=20 dB, and MDL=20 dB. We observe a sharp cutoff on the left side of the histogram. Transmission at a rate smaller than this cutoff capacity will be perfectly secure independent of the channel realization. However, if the legitimate channel users choose to communicate at a rate R higher than this cutoff, there is a finite probability that the eavesdropper can (at least in principle) learn something about the secret information. We call this probability the *probability of interception* $p_{int}(R) = \text{Prob}[C_s < R]$. Instead of lowering the transmission rate to such a value that perfect secrecy is always attained, we adopt a different strategy. Similar to the outage approach in communication systems, we let the transmitter send information at a rate such that there is a (small) probability of interception. We refer to the associate maximal secrecy rate as the *outage secrecy capacity*, which can be obtained via the statistical distribution (histogram) of the secrecy capacity C_s . We plot the probability of interception vs. the outage secrecy capacity in Fig. 2(b), which shows the trade-off between transmission rate and security.

In [11], we show that even if an eavesdropper introduces only 5 dB of MDL, we can still have about 7%-20% of the aggregated per-mode fiber capacity in perfect secrecy 99.99% of the time. Using just a single wavelength channel modulated at 100 Gb/s per spatial mode already yields a secrecy capacity that is orders of magnitude higher way than what is achievable through QKD.

C. The optimality of $\mathbf{Q_x} = P_0 I$

In this section, we use both analyses and simulations to justify the conjecture that $\mathbf{Q_x} = P_0 I$ is the optimum power allocation strategy under the assumption of an uninformed transmitter. We first show that we can greatly reduce the solution space of the optimization problem (3) by considering

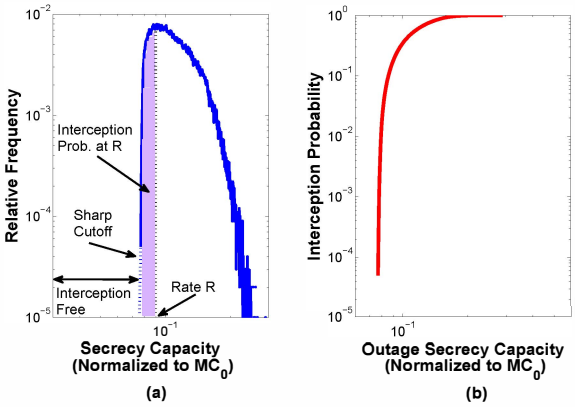

Fig. 2. (a) Histogram of the secrecy capacity (normalized to MC_0) based on 10^5 random realizations; (b) Interception probability as a function of outage secrecy capacity.

only diagonal covariance matrices. This follows from:

$$\begin{aligned}
& I(x,y) - I(x,y^e) \\
= \;& \log_2\left[\det(\mathbf{I} + \text{SNR}\mathbf{U}\mathbf{Q_x}\mathbf{U}^\dagger)\right] \\
& - \log_2\left[\det(\mathbf{I} + \text{SNR}^e\sqrt{\mathbf{V^e}}\mathbf{U^e}\mathbf{Q_x}\mathbf{U^{e\dagger}}\sqrt{\mathbf{V^e}})\right] \\
= \;& \log_2\left[\det(\mathbf{I} + \text{SNR}\mathbf{U}\mathbf{W}\mathbf{\Lambda^Q}\mathbf{W}^\dagger\mathbf{U}^\dagger)\right] \\
& - \log_2\left[\det(\mathbf{I} + \text{SNR}^e\sqrt{\mathbf{V^e}}\mathbf{U^e}\mathbf{W}\mathbf{\Lambda^Q}\mathbf{W}^\dagger\mathbf{U^{e\dagger}}\sqrt{\mathbf{V^e}})\right] \\
= \;& \log_2\left[\det(\mathbf{I} + \text{SNR}(\mathbf{UW})\mathbf{\Lambda^Q}(\mathbf{W}^\dagger\mathbf{U}^\dagger))\right] \\
& - \log_2\left[\det(\mathbf{I} + \text{SNR}^e\sqrt{\mathbf{V^e}}(\mathbf{U^eW})\mathbf{\Lambda^Q}(\mathbf{W}^\dagger\mathbf{U^{e\dagger}})\sqrt{\mathbf{V^e}})\right] \\
= \;& \log_2\left[\det(\mathbf{I} + \text{SNR}\widetilde{\mathbf{U}}\mathbf{\Lambda^Q}\widetilde{\mathbf{U}}^\dagger)\right] \\
& - \log_2\left[\det(\mathbf{I} + \text{SNR}^e\sqrt{\mathbf{V^e}}\widetilde{\mathbf{U}}^\mathbf{e}\mathbf{\Lambda^Q}\widetilde{\mathbf{U}}^{\mathbf{e}\dagger}\sqrt{\mathbf{V^e}})\right]. \quad (6)
\end{aligned}$$

In the above equations, the first equality follows from the unitary and MDL channel models for legitimate receiver and eavesdropper. That is, $\mathbf{H} = \mathbf{U}$ and $\mathbf{H^e} = \mathbf{U^e}\sqrt{\mathbf{V^e}}$. The second equality follows from the singular value decomposition $\mathbf{Q_x} = \mathbf{W}\mathbf{\Lambda^Q}\mathbf{W}^\dagger$, where $\mathbf{W}$ is a unitary matrix and $\mathbf{\Lambda^Q}$ is a diagonal matrix. The third and fourth equalities follow from that the product of two unitary matrices ($\widetilde{\mathbf{U}} = \mathbf{UW}$ or $\widetilde{\mathbf{U}}^\mathbf{e} = \mathbf{U^eW}$) is also unitary. Note that all the statistical characteristics of $\mathbf{Q_x}$ are captured by $\mathbf{\Lambda^Q}$ as the result of our channel models. Also, since $\mathbf{U}$, $\mathbf{U^e}$, and $\mathbf{W}$ are independent, the statistical characteristics of $\mathbf{U}$ and $\mathbf{U^e}$ are preserved in $\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{U}}^\mathbf{e}$, respectively.

Next, we study the interception probability vs. outage secrecy capacity for different diagonal matrices $\mathbf{\Lambda^Q}$. In particular, we focus on the following search scenarios:

- Exhaustive search with a quantized step size: the full power of P_0 is quantized to l levels with a step size of P_0/l. Power allocation on a spatial mode can only take values of kP_0/l, with $k = 1, 2, ..., l$. We exhaustively evaluate all the possible power levels kP_0/l assigned to M modes. This is equivalent to testing all M-combinations with repetitions from a set of L distinctive

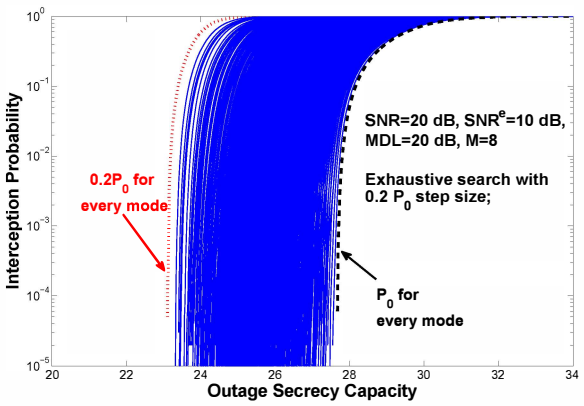

Fig. 3. Interception probability vs. outage secrecy capacity for exhaustive search with a step size of $0.2P_0$, $M = 8$, MDL= 20 dB, SNR=20 dB, and SNR^e=10 dB.

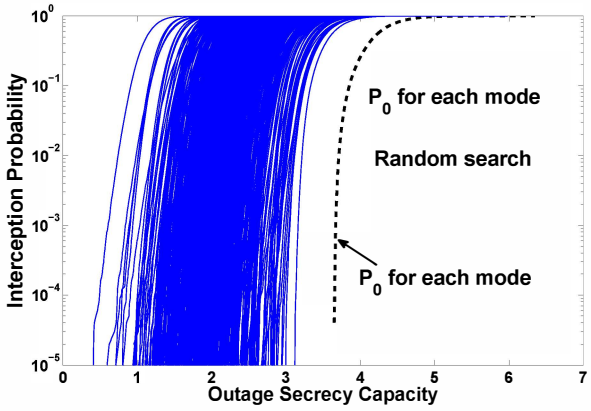

Fig. 4. Interception probability vs. outage secrecy capacity for random search wiht $M = 8$, MDL= 20 dB, SNR=3 dB, and SNR^e=1dB.

elements. The total number of cases tested for a given l and M is given by $\binom{l+M-1}{M}$.

- Random search: the values of the diagonal elements of $\mathbf{\Lambda}^{\mathbf{Q}}$ are randomly drawn for a uniform distribution $[0, P_0]$.

Fig. 3 shows the results of all the cases (in blue) from exhaustive searches with a step size of $0.2P_0$ ($l = 5$) for $M = 8$, MDL=20 dB, SNR=20 dB, and SNR^e=10 dB. The plots show that allocating P_0 to every spatial mode is optimal in the sense that for the same interception probability the outage secrecy capacity achieved by this scheme is larger than that of any other scheme (as shown by the black dashed curve). We also note that allocating $0.2P_0$ to every mode is the least favorable strategy – the secrecy capacity for a given interception probability is smaller than that of any other scheme (as shown by the red dotted curve). Fig. 4 shows the results (in blue) from 500 cases of random search, with $M = 8$, MDL=20 dB, SNR=3 dB, and SNR^e=1 dB. It is obvious that allocating P_0 to every mode again has the best performance (as shown by the black dashed curve). We run extensive tests using the combinations of scenarios and different values of M, MDL, SNR, and SNR^e. All the results obtained so far indeed support the claim that uncorrelated and equal power allocation of P_0 to all the modes is optimal in terms of interception probability performance. A rigorous proof will be reported in our future work.

IV. Rate-Distortion Analysis

In addition to equivocation, we also consider distortion as a measure of secrecy. Our ultimate goal is to design coding or encryption schemes for MIMO-SDM systems so that the eavesdropper, even equipped with unlimited computing power, cannot make a close enough estimation of the source under a given distortion measure. As such, secrecy under distortion [15] provides an operational measure by comparing the difference between the information intended for the legitimate receiver and the eavesdroppers estimation. Here, we focus on the Hamming distortion (which is the same as the bit

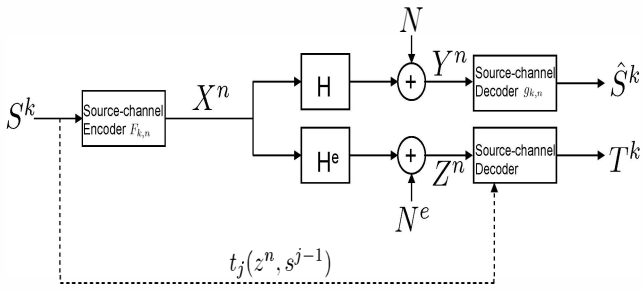

Fig. 5. The joint source-channel model.

error rate (BER) for a binary source) and formulate a joint source-channel problem. The system model is shown in Fig. 5. The transmitter sends an i.i.d. source sequence S^k with the objective of keeping the average distortion between the eavesdropper's estimation T^k and the sequence S^k as high as possible. We evaluate the tradeoff between the transmission rate R (symbols/channel use) and the distortion D of the eavesdropper's estimation under the worst case scenario in which a very capable eavesdropper not only has the information by wiretapping the channel but also knows the past realization of the source S^{j-1} at each time j to assist the estimation of the current symbol S_j. Mathematically, the Hamming distortion between the symbols S_i and $\widehat{S}_i$ is given by:

$$d(S_i, \widehat{S}_i) = \begin{cases} 1, & \text{if } S_i = \widehat{S}_i; \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

In addition, the Hamming distortion between the symbols S^k and $\widehat{S}^k$ is given by:

$$D(S^k, \widehat{S}^k) = \frac{1}{k} \sum_{i=1}^{k} d(S_i, \widehat{S}_i). \tag{8}$$

Based on the results of [16], we obtain the distortion as a function of achievable rate for the transmission of i.i.d. Bernoulli sequences with $p = 0.3$ and $p = 0.5$, as shown

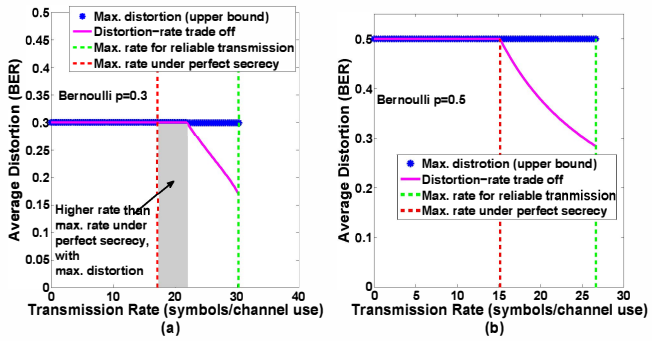

Fig. 6. Avg. distortion vs. achievable rate: the Bernoulli source with $p = 0.3$ (a) and $p = 0.5$ (b).

in Fig.6 (a) and (b), respectively. In particular, we consider a four-mode ($M = 4$) MIMO-SDM system with a uniform MDL model (MDL=20 dB, SNR=20 dB, SNR^e=10 dB). In Fig. 6, the maximum distortion for each source sequence is shown in blue. The green and red vertical lines represent the maximum allowable rate for reliable transmission and the maximum allowable rate under perfect secrecy, respectively. The purple solid curve depicts the tradeoff between distortion and achievable rate. For a biased source such as the Bernoulli $p = 0.3$ sequences, the transmitter can operate at a higher rate than the maximal allowable rate under perfect secrecy, while ensuring the maximum amount of distortion for the eavesdropper (as shown in the shaded region of Fig. 6 (a)). For an unbiased source (the Bernoulli $p = 0.5$ sequences), the transmitter can operate only as high as the maximal allowable rate under perfect secrecy to ensure maximal distortion for the eavesdropper. Nevertheless, relatively large distortion values (i.e., high eavesdropper BERs) can be achieved at significantly larger secret transmission rates.

V. Conclusions

In this work, we evaluated the security benefits of the SDM using both equivocation and distortion as measures of secrecy. We first focus on the optimal power allocation strategy under the assumption of uninformed transmitters. Based on analyses and extensive simulations, we substantiate our claim that allocating maximal allowable power to each mode is optimal. Motivated by our goal to ultimately design coding schemes that can maximize the eavesdropper's estimation error, we apply joint source-channel coding and quantify the rate-distortion tradeoff.

VI. Acknowledgement

Eva. C. Song would like to acknowledge the support from National Science Foundation under the Grant CCF-1116013 and the Grant CNS-09-05086.

References

[1] K. Shaneman, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention," MILCOM 2004, vol. 2, pp.711, Oct. 2004.

[2] V. Scarani et al.,"The security of practical quantum key distribution," Rev. Mod. Phys, vol. 81, no. 3, pp. 1301-1350, July-Sept. 2009.

[3] A. R. Dixon, et al., "Continuous operation of high bit rate quantum key distribution," Appl. Phys. Lett. vol. 96, pp. 161102, 2010.

[4] N. Peters, et al., "Quantum communications in reconfigurable optical networks: DWDM QKD through a ROADM," OFC 2010, paper OTuk1, Mar. 2010.

[5] R.-J. Essiambre, "Capacity limits of fiber optical networks," Journal of Lightwave Technologies, vol. 28, no. 4, pp. 662-701, Feb. 2010.

[6] P. J. Winzer, "Energy-efficient optical transport capacity scaling through spatial multiplexing," IEEE Photon. Technol. Lett., vol. 23, pp.851-853, 2011.

[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] S. Chandrasekhar et al.,"WDM/SDM Transmission of 10 x 128-Gb/s PDM-QPSK over 2688-km 7-Core Fiber with a per-Fiber Net Aggregate Spectral-Efficiency Distance Product of 40,320 km.b/s/Hz", ECOC 2011, Th.13.C.4, Sept. 2011.

[9] R. Ryf et al.,"Analysis of mode-dependent gain in raman amplified few-mode fiber," OFC 2012, OW1D.1, Mar. 2012.

[10] S. Randel et al., "Adaptive MIMO signal processing for mode-division multiplexing," OFC 2012, OW3D.5, Mar. 2012.

[11] K. Guan, P. J. Winzer, and E. Soljanin, "Information-theoretic security in space-division multiplexed fiber optic networks," ECOC 2012, Tu.3.C.4, Sep. 2012.

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

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

[14] 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.

[15] H. Yamamoto, "Rate-distortion theory for the Shannon cipher cystem," IEEE Trans. Inf. Theory, vol.43, no. 3, pp. 827-835, May 1997.

[16] C. Shieler et al., "Source-channel secrecy with causal disclosure," Allerton Conference, 2012.