On Secrecy Rate Analysis of Spatial Modulation and Space Shift Keying

Sina Rezaei Aghdam Tolga M. Duman
Dept. of Electrical and Electronics Engineering
Bilkent University
Ankara, Turkey, TR 06800
Email: {aghdam, duman}@ee.bilkent.edu.tr

Marco Di Renzo
Paris-Saclay University
Laboratory of Signals and Systems (UMR-8506)
CNRS/CentraleSupelec/University Paris-Sud XI, France
Email: marco.direnzo@lss.supelec.fr

***Abstract*—Spatial modulation (SM) and space shift keying (SSK) represent transmission methods for low-complexity implementation of multiple-input multiple-output (MIMO) wireless systems in which antenna indices are employed for data transmission. In this paper, we focus our attention on the secrecy behavior of SSK and SM. Using an information-theoretic framework, we derive expressions for the mutual information and consequently compute achievable secrecy rates for SSK and SM via numerical evaluations. We also characterize the secrecy behavior of SSK by showing the effects of increasing the number of antennas at the transmitter as well as the number of antennas at the legitimate receiver and the eavesdropper. We further evaluate the secrecy rates achieved by SM with different sizes of the underlying signal constellation and compare the secrecy performance of this scheme with those of general MIMO and SIMO systems. The proposed framework unveils that SM is capable of achieving higher secrecy rates than the conventional single-antenna transmission schemes. However, it underperfoms compared to a general MIMO system in terms of the achievable secrecy rates.**

Index Terms — Physical layer security, MIMO wiretap channel, spatial modulation, space shift keying, secrecy capacity.

I. Introduction

Multiple-input multiple-output (MIMO) systems are designed to either increase the capacity or to enhance the reliability of wireless links [1]. This enhancement is attained at the price of higher complexity, increased hardware requirements and higher power consumption due to the need for multiple radio-frequency (RF) chains. Spatial modulation (SM) and space shift keying (SSK) are relatively new MIMO transmission schemes in which only one of the transmit antennas is active at each time instant. By employing these transmission schemes spatial multiplexing gains can be achieved with a reduced complexity and a smaller power consumption due to the fact that ideally a single RF chain is required at the transmitter [2]. The key idea in SM and SSK is to encode the information bits into the index of the activated antenna. While antenna indices are the only information-carrying units in SSK [3], SM takes advantage of a conventional amplitude or phase modulation along with the antenna indices to transmit data [4].

Even though the performances of SSK and SM have been extensively studied for different scenarios [5]- [6], very limited attention has been paid to the secrecy behavior of these schemes. The fundamental setup in physical layer security has been introduced by Wyner in [7], where secure communication has been studied over a wiretap channel in the presence of an eavesdropper. It was shown in [7] that confidential messages can be transmitted securely without using an encryption key if the channel capacity of the link from source to the legitimate receiver is higher than that of the wiretap link. In subsequent literature, Wyner's results have been extended to other scenarios such as Gaussian wiretap channels [8]. More recently, the emergence and increasing pervasiveness of wireless communication systems have spurred considerable interest in investigation of these systems in the context of secure communications [9]. As an intuitive extension, the information theoretic secrecy capacity of MIMO communication systems has been analyzed in [10] and [11]. More specifically, it has been proved in [11] that for an arbitrary number of transmit/receive antennas, the secrecy capacity is the difference of the two mutual information terms, i.e. that of the legitimate receiver minus that of the eavesdropper, after a suitable optimization over the input covariance matrix.

An initial study of the secrecy capacity of SM has been provided in [12] where the contribution of the spatial component in the overall capacity has been neglected. The secrecy capacity of the spatial component of SM and SSK systems has been characterized in a semi-analytical fashion in [13], where the error probabilities of SSK, which are obtained via simulations, have been used in the expression for secrecy capacity of the binary symmetric channel (BSC).

As the study in [13] is limited to a system with two transmit antennas and it is only semi-analytical and approximate, here we propose an analytic framework which allows us to give a characterization of the secrecy behavior of SSK systems with different number of transmit and receive antennas. To this end, with the assumption that the antennas are equally likely to be activated, we define an achievable secrecy rate as the difference of the mutual information quantities corresponding to the legitimate receiver's and the eavesdropper's channels. Then, we derive an expression for the mutual information of SSK and extend it to the more general case of SM. For both SSK and SM we characterize the above-mentioned achievable secrecy rates via numerical evaluations applied on the derived mutual information expressions.

The paper is organized as follows. Section II introduces our system model and explains the definition of the secrecy rate.

978-1-4799-8505-0/15/$31.00 ©2015 IEEE

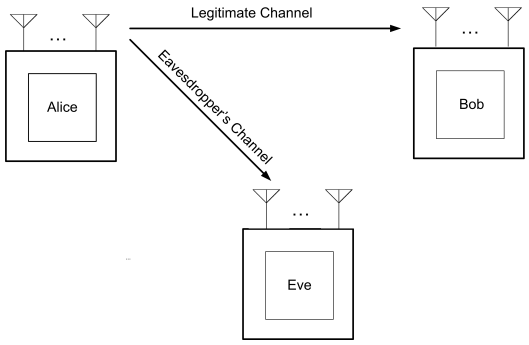

Fig. 1: The MIMOME secrecy model.

In Section III, we derive expressions for the corresponding mutual information terms. Numerical results are provided in Section IV, and we conclude the paper in Section V.

II. System Model

We consider a general multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) wiretap channel as depicted in Fig. 1. While Alice transmits a spatially modulated signal to the legitimate receiver, Bob, a third party, Eve, is present with capability of eavesdropping on Alice's signal. Alice, Bob and Eve are assumed to be equipped with N_t, N_{r_b} and N_{r_e} antennas, respectively. In this section, we formulate the received signals and also define an achievable secrecy rate for two separate cases where SSK and SM are employed at the transmitter.

The notation of this paper is as follows. Scalars and vectors are denoted with the lowercase letters. Uppercase letters are used to represent matrices. Random variables are denoted with the boldface letters. The expectation value and the probability mass (or density) function of a random variable $\mathbf{a}$ are represented by $\mathbb{E}_{\mathbf{A}}\{.\}$ and $P_{\mathbf{A}}(.)$, respectively. Moreover, $(.)^H$ and $\| \, . \, \|_F$ denote Hermitian and Frobenius norm operations.

A. Space Shift Keying

By employing SSK at the transmitter, the received signals y and z at the legitimate receiver and eavesdropper can be represented, respectively, as

$$\mathbf{y} = \mathbf{H}_b\mathbf{x} + \mathbf{n}_y \tag{1}$$

$$\mathbf{z} = \mathbf{H}_e\mathbf{x} + \mathbf{n}_z, \tag{2}$$

where, $\mathbf{x} \in \{x_1, x_2, ..., x_{N_t}\}$ is the SSK signal vector which is of the form

$$x_m = [0 \; 0 \; ... \; 1 \; ... \; 0 \; 0],$$
$$\uparrow$$
$$m^{th} \text{ element}$$

with the position of "1" indicating the antenna being activated. $\mathbf{n}_y$ and $\mathbf{n}_z$ are independent and identically distributed (i.i.d.) additive white Gaussian noise terms which follow circularly symmetric complex Gaussian distributions, $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_y})$ and $\mathcal{CN}(0, \sigma^2_{\mathbf{n}_z})$, respectively. $\mathbf{H}_b$ and $\mathbf{H}_e$ are the channel matrices corresponding to the legitimate channel and the eavesdropper's channel, respectively. The elements of the channel matrices are i.i.d. with distribution $\mathcal{CN}(0, 1)$. Furthermore, $\mathbf{H}_b$, $\mathbf{H}_e$, $\mathbf{n}_y$ and $\mathbf{n}_z$ are independent. It is assumed that the fading process is ergodic. The legitimate receiver and the eavesdropper know their own channels perfectly. However, no channel state information is available at the transmitter.

Secrecy capacity can be defined as the rate at which transmitter can use the main link so as to deliver its message to the legitimate receiver in a way that the eavesdropper cannot successfully decode the same information. Based on [14], when $\sigma^2_{\mathbf{n}_y} < \sigma^2_{\mathbf{n}_z}$ and $N_{r_e} \leq N_{r_b}$, the MIMOME secrecy capacity can be calculated as:

$$C_s = \max_{P_{\mathbf{X}}(x)} \big(I(\mathbf{x}; \mathbf{y}|\mathbf{H}_b) - I(\mathbf{x}; \mathbf{z}|\mathbf{H}_e) \big), \tag{3}$$

where the optimization is over the input distribution. It is well known that for a symmetric discrete memoryless channel, mutual information is maximized with equiprobable inputs [15, p. 94]. With a similar reasoning, it can be claimed that the maximum of $I(\mathbf{x}; \mathbf{y}|\mathbf{H})$ is achieved with a source with equiprobable inputs. Here, we define an achievable secrecy rate as

$$R_s^{SSK} = \big[I(\mathbf{x}; \mathbf{y}|\mathbf{H}_b) - I(\mathbf{x}; \mathbf{z}|\mathbf{H}_e) \big]\big|_{P_{\mathbf{X}}(x)=1/N_t}, \tag{4}$$

if $I(\mathbf{x}; \mathbf{y}|\mathbf{H}_b) < I(\mathbf{x}; \mathbf{z}|\mathbf{H}_e)$ and zero otherwise. This quantifies the information being secretly transmitted with the assumption that the active antennas are selected equiprobably. Indeed, R_s^{SSK} is simply a lower bound on the secrecy capacity given in (3) in view of the fact that $P_{\mathbf{X}}(x) = 1/N_t$ is not necessarily the input distribution which maximizes the expression in (3).

B. Spatial Modulation

While the antenna indices are the only source of information in SSK transmission, SM additionally employs an amplitude or phase modulation scheme. In this case, the received signals at the legitimate receiver and the eavesdropper can be written as:

$$\mathbf{y}' = \mathbf{H}_b\mathbf{x}\mathbf{s} + \mathbf{n}_{y'} \tag{5}$$

$$\mathbf{z}' = \mathbf{H}_e\mathbf{x}\mathbf{s} + \mathbf{n}_{z'}, \tag{6}$$

where $\mathbf{s} \in \{s_1, s_2, ..., s_N\}$ denotes the symbol chosen from an equiprobable discrete signal constellation with size N. We assume that a power constraint of unity, i.e., $\mathbb{E}\{|\mathbf{s}|^2\} = 1$, holds. In this case, the achievable secrecy rate can be defined as

$$R_s^{SM} = \big[I(\mathbf{x}, \mathbf{s}; \mathbf{y}'|\mathbf{H}_b) - I(\mathbf{x}, \mathbf{s}; \mathbf{z}'|\mathbf{H}_e) \big]\big|_{P_{\mathbf{X}}(x)=1/N_t, P_{\mathbf{S}}(s)=1/N}, \tag{7}$$

which is the difference between the mutual information terms corresponding to the legitimate receiver and the eavesdropper with the assumption that the amplitude or phase modulation symbols are selected equiprobably, $P_{\mathbf{S}}(s) = 1/N$, along with the same assumption for the antenna indices, i.e., $P_{\mathbf{X}}(x) = 1/N_t$.

III. Mutual Information and Secrecy Rate

In this section, we separately derive expressions for the mutual information of SSK and SM. These expressions make possible the evaluation of the secrecy rates in (4) and (7).

A. Space Shift Keying

So as to characterize the secrecy rate of SSK, we are required to evaluate the mutual information between the source and the destination, i.e., $I(\mathbf{x};\mathbf{y}|\mathbf{H}_b)$, as well as the mutual information between the source and the eavesdropper, i.e., $I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)$. For $N_r \times N_t$ MIMO channel, $\mathbf{H} \sim \mathcal{CN}(0,1)$, mutual information can be calculated using the following formula [16, Eq. (2.28)]:

$$I(\mathbf{x};\mathbf{y}|\mathbf{H}) = \mathbb{E}_{\mathbf{H}}\Bigg\{ \sum_{x\in\mathbf{X}} \int_y P_{\mathbf{XY}|\mathbf{H}}(x,y|\mathbf{H}) \times \log \frac{P_{\mathbf{XY}|\mathbf{H}}(x,y|\mathbf{H})}{P_{\mathbf{X}|\mathbf{H}}(x|\mathbf{H}) P_{\mathbf{Y}|\mathbf{H}}(y|\mathbf{H})}\, dy \Bigg\}. \quad (8)$$

The N_r-dimensional received signal follows a complex Gaussian distribution with conditional probability density function (PDF) given by:

$$P_{\mathbf{Y}|\mathbf{XH}}(y|x_m,H) = \frac{1}{\pi^{N_r}\sigma_n^{2N_r}} \times \exp(-\parallel y - Hx_m \parallel_F^2 / \sigma_n^2). \quad (9)$$

As stated in the previous section we assume that the antennas are selected equiprobably, i.e., $P_{\mathbf{X}}(x) = \frac{1}{N_t}$. Note that this is due to the fact that in the absence of channel state information at the transmitter (CSIT), the active antenna sets are equally likely to be used. We obtain

$$P_{\mathbf{XY}|\mathbf{H}}(x_m,y|H) = \frac{1}{N_t} P_{\mathbf{Y}|\mathbf{XH}}(y|x_m,H), \quad (10)$$

$$P_{\mathbf{X}|\mathbf{H}}(x|H) = \frac{1}{N_t}, \quad (11)$$

$$P_{\mathbf{Y}|\mathbf{H}}(y|H) = \frac{1}{N_t} \sum_{m=1}^{N_t} P_{\mathbf{Y}|\mathbf{XH}}(y|x_m,H). \quad (12)$$

By substituting (9)-(12) in (8), the mutual information for SSK can be derived as:

$$I(\mathbf{x};\mathbf{y}|\mathbf{H}) = \mathbb{E}_{\mathbf{H}}\Bigg\{ \frac{1}{N_t\pi^{N_r}\sigma_n^{2N_r}} \times \sum_{m=1}^{N_t} \int_y \exp(-\parallel y - \mathbf{H}x_m \parallel_F^2 / \sigma_n^2) \times \log \frac{N_t \exp(-\parallel y - \mathbf{H}x_m \parallel_F^2 / \sigma_n^2)}{\sum_{m'=1}^{N_t} \exp(-\parallel \mathbf{y} - \mathbf{H}x_{m'} \parallel_F^2 / \sigma_n^2)}\, dy \Bigg\}. \quad (13)$$

B. Spatial Modulation

For SM, the mutual information between the two inputs and the output can be written by using the chain rule [16, Eq. 2.62], as:

$$I(\mathbf{x},\mathbf{s};\mathbf{y}'|\mathbf{H}) = I(\mathbf{x};\mathbf{y}'|\mathbf{H}) + I(\mathbf{s};\mathbf{y}'|\mathbf{x},\mathbf{H}). \quad (14)$$

The term $I(\mathbf{x};\mathbf{y}'|\mathbf{H})$ is simply the mutual information for SSK which is given in (13). The second term, i.e. $I(\mathbf{s};\mathbf{y}'|\mathbf{x},\mathbf{H})$, can be calculated similar to (8), as

$$I(\mathbf{s};\mathbf{y}'|\mathbf{x},\mathbf{H}) = \mathbb{E}_{\mathbf{XH}}\Bigg\{ \sum_{s\in\mathbf{S}} \int_{y'} P_{\mathbf{SY}'|\mathbf{XH}}(s,y'|\mathbf{x},\mathbf{H}) \times \log \frac{P_{\mathbf{SY}'|\mathbf{XH}}(s,y'|\mathbf{x},\mathbf{H})}{P_{\mathbf{S}|\mathbf{XH}}(s|\mathbf{x},\mathbf{H}) P_{\mathbf{Y}'|\mathbf{XH}}(y'|\mathbf{x},\mathbf{H})}\, dy' \Bigg\}. \quad (15)$$

We can write

$$P_{\mathbf{SY}'|\mathbf{XH}}(s_n,y'|x,H) = \frac{1}{N} P_{\mathbf{Y}'|\mathbf{SXH}}(y'|s_n,x,H), \quad (16)$$

$$P_{\mathbf{S}|\mathbf{XH}}(s_n|x,H) = \frac{1}{N}, \quad (17)$$

$$P_{\mathbf{Y}'|\mathbf{XH}}(y'|x,H) = \frac{1}{N} \sum_{n=1}^{N} P_{\mathbf{Y}'|\mathbf{SXH}}(y'|s_n,x,H), \quad (18)$$

where,

$$P_{\mathbf{Y}'|\mathbf{SXH}}(y'|s_n,x,H) = \frac{1}{\pi^{N_r}\sigma_n^{2N_r}} \times \exp(-\parallel y' - Hxs_n \parallel_F^2 / \sigma_n^2). \quad (19)$$

By substitution of the conditional PDFs above in (15) we have

$$I(\mathbf{s};\mathbf{y}'|\mathbf{x},\mathbf{H}) = \mathbb{E}_{\mathbf{XH}}\Bigg\{ \frac{1}{N\pi^{N_r}\sigma_n^{2N_r}} \times \sum_{n=1}^{N} \int_{y'} \exp(-\parallel y' - \mathbf{H}\mathbf{x}s_n \parallel_F^2 / \sigma_n^2) \times \log \frac{N \exp(-\parallel y' - \mathbf{H}\mathbf{x}s_n \parallel_F^2 / \sigma_n^2)}{\sum_{n'=1}^{N} \exp(-\parallel y' - \mathbf{H}\mathbf{x}s_{n'} \parallel_F^2 / \sigma_n^2)}\, dy' \Bigg\}. \quad (20)$$

According to (14), the mutual information for SM is equal to the summation of the terms in (13) and (20). Namely, the overall mutual information has two components; one associated with the spatial component and the other corresponding to the conventional modulation bits. Hence by employing SM instead of SSK, we can increase the mutual information by the amount of mutual information corresponding to the radiated symbol, i.e., $I(\mathbf{s};\mathbf{y}'|\mathbf{x},\mathbf{H})$. While the higher rate of SM with respect to SSK is expected, secrecy behavior of these two transmission schemes requires further investigation as explored in Section IV.

IV. Numerical Examples

In this section, we quantify the achievable secrecy rate of SSK and SM. For SSK, the secrecy rate is calculated using (4) and by numerically evaluating the mutual information expression given in (13), for the main channel and the eavesdropper's channel. Fig. 2 depicts the secrecy rate for the case with a single receive antenna at the legitimate receiver and the eavesdropper. This rate is evaluated via subtracting the mutual information associated with the eavesdropper's channel from the mutual information corresponding to the legitimate user's channel. In this evaluation, by considering i.i.d. channel coefficients from different transmit antennas, the secrecy rate is averaged over many channel realizations and

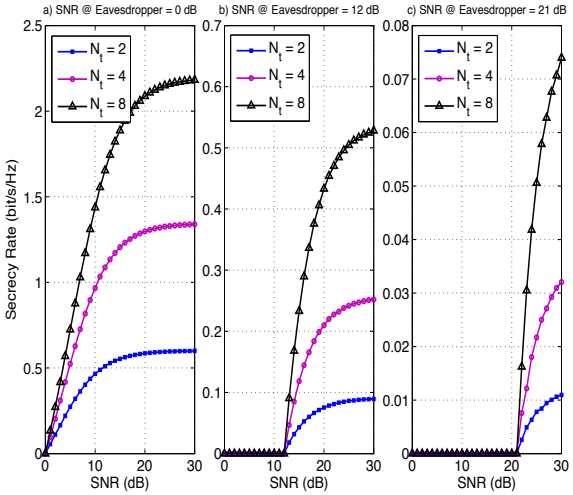

Fig. 2: Secrecy rate for a SSK system with different number of transmit antennas. $N_{r_e} = N_{r_b} = 1$.

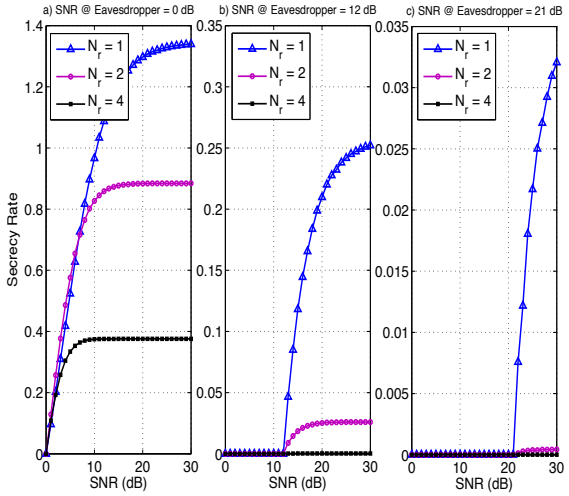

Fig. 3: Secrecy rate for a SSK system with different number of receiver antennas at the legitimate receiver and the eavesdropper. $N_t = 4, N_{r_e} = N_{r_b} = N_r$.

plotted versus legitimate user's signal to noise ratio (SNR), while it is assumed that the eavesdropper's SNR is fixed at 0, 12 and 21 dB. It can be inferred from Fig. 2 that for the case where eavesdropper's SNR is fixed to 0 dB, increasing the number of transmit antennas from 2 to 4 and 8 gives rise to 1 and 2 bits/s/Hz enhancement in the secrecy rate, respectively.

By comparing the Figures 2-(a) , 2-(b) and 2-(c), it can be observed that the secrecy rates are decreased when we increase the SNR at the eavesdropper. This is to be expected due to the fact that by increasing the Eve's SNR, we decrease the gap between Bob's and Eve's SNRs and this gives rise to a smaller difference between the corresponding mutual informations. Furthermore, it is inferred that for the cases where Eve has higher SNRs, the advantages of larger number of transmit antennas is more apparent.

The effects of increasing the number of receive antennas is shown in Fig. 3. Four antennas have been considered at the transmitter and the secrecy capacity has been evaluated by varying the legitimate receiver's SNR for three cases where the eavesdropper's SNR is fixed at 0, 12 and 21 dB, respectively. These results declare that increasing the number of antennas at the legitimate receiver and the eavesdropper results in a decreased secrecy level. This behavior is different from the capacity behavior of SSK in the sense that a higher number of receive antennas results in an increased achievable information rate (see, e.g., Fig. 5 in [18]). This is due to the fact that increasing the number of receive antennas at the legitimate receiver and the eavesdropper leads to a capacity gain for both of the receivers and as a result the behavior of secrecy capacity differs from that of capacity.

In order to characterize the secrecy behavior of SM, we quantify the secrecy rate using (7) and via numerical evaluations of the mutual information expressions for the main channel and the eavesdropper's channel, given in (20). Fig. 4 shows the secrecy rate for SM. It can be observed that SM provides larger secrecy rates than SSK. Also, by increasing the size of the underlying signal constellation, namely N, a better performance is attained for SM. This is due to the fact that in SM, utilization of a conventional modulation along with encoding of the data in the antenna index introduces a further randomization which enhances the achievable secrecy rate. Similar to the case for SSK, when Eve's SNR is higher, SM's secrecy rates are decreased. In these conditions, system benefits more from the increased signal constellation size.

What we can recognize from Fig. 4 is that for a fixed number of transmit antennas, employing an amplitude or phase modulation along with the spatial encoding of data can increase the secrecy rate. This increased secrecy rate is attained

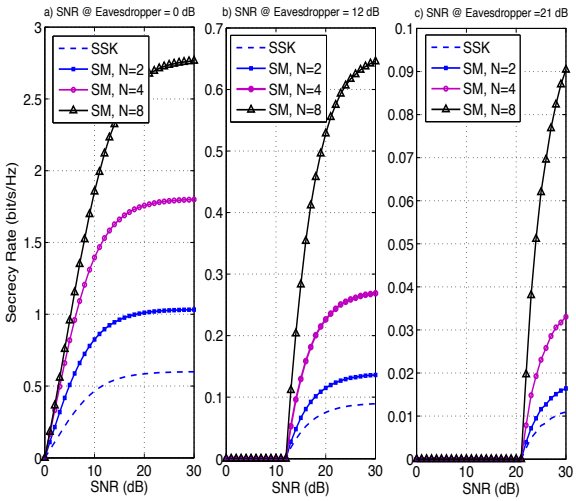

Fig. 4: Secrecy rate for a SM system with different underlying signal constellations. $N_t = 2$, $N_{r_e} = N_{r_b} = 1$.

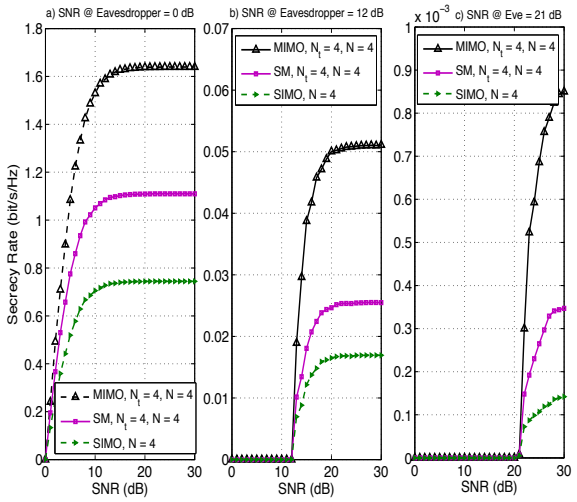

Fig. 5: Comparison of secrecy rates for SM and general MIMO and SIMO systems. $N = 4$, $N_{r_e} = N_{r_b} = 2$.

at the price of increased detection complexity and higher bit error rates (BERs). This is because increasing the order of modulation which is advantageous from a secrecy perspective, on the other hand, gives rise to a decreased minimum distance between the points in the signal-constellation and results in a higher probability of error.

In Fig. 5 the secrecy rates of SM have been compared to those of general MIMO and SIMO systems with finite alphabet inputs with $N = 4$, namely, using quadrature phase shift keying (QPSK) transmission. The results for the general MIMO have been obtained using [19, Eq. (5)]. Fig. 5 clearly shows that SM can yield an improved secrecy performance with respect to the SIMO case due to taking advantage of multiple transmit antennas. Yet, its secrecy rate is notably less than a general MIMO transmission where all of the transmitted antennas are activated. In fact, this degradation is the price that should be paid to take advantage of appealing features of SM in terms of complexity and cost.

V. Conclusion

In this paper, we derived expressions for achievable secrecy rates for SSK and SM using an information-theoretic framework. We then studied the secrecy behavior of these low-complexity MIMO transmission schemes for different number of transmit and receive antennas, and for different sizes of underlying signal constellation. Moreover, we compared the secrecy rates achieved by SM with those of general SIMO and MIMO systems. Our results show that SM is capable of achieving a better secrecy rate with respect to a single-antenna transmission. However, there is a gap between the secrecy rates of SM and a general MIMO system in which all transmit antennas are activated in each time instant. The framework proposed in this paper can serve as a basis for future studies on spatial encoding of data in the context of secure wireless communications.

Acknowledgment

This work is supported by the Scientific and Technical Research Council of Turkey (TUBITAK) under grant #113E223 and the European Commission under the grant NEWCOM #318306.

References

[1] T. M. Duman and A. Ghrayeb, Coding for MIMO Communication Systems. Wiley, 2008.

[2] A. Stavridis, S. Sinanovic, M. Di Renzo, and H. Haas, "Energy evaluation of spatial modulation at a multiantenna base station", *IEEE Veh. Technol. Conf.– Fall*, pp. 1–5, Sep. 2013.

[3] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3692–3703, 2009.

[4] R. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228-2241, July 2008.

[5] M. Di Renzo, H. Haas, and P. M. Grant, "Spatial modulation for multipleantenna wireless systems – A survey," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 182-191, Dec. 2011.

[6] M. Di Renzo, H. Haas, and A. Ghrayeb, S. Suguira, L. Hanzo "Spatial modulation for generalized MIMO: challenges, opportunities and implementation," *Proc. IEEE*, vol. 102, no. 1, pp. 56–103, 2014.

[7] A. Wyner, "The Wire-tap Channel," *Bell. Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451-456, July 1978.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, Special Issue on Information Theoretic Security, vol. 54, pp. 2515–2534, June 2008.

[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, pp. 5515–5532, Nov. 2010.

[11] F. Oggier, B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[12] S. Sinanovic, M. Di Renzo, and H. Haas, "Secrecy rate of time switched transmit diversity system," in *Proc., IEEE Veh. Technol. Conf. (VTC)* , pp. 1–5, May 2011.

[13] M. Di Renzo, H. Haas, N. Serafimovski, S. Sinanovic, "Secrecy capacity of space keying with two antennas," *IEEE Veh. Technol. Conf.*, pp. 1-5, Fall 2012.

[14] S.-C. Lin and P.-H. Lin, "On Secrecy Capacity of Fast Fading MIMOME Wiretap Channels with Statistical CSIT," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3293 – 3306, Jun. 2014.

[15] R. Gallager, *Information Theory and Reliable Communications.* New York: Wiley, 1968.

[16] T. M. Cover and J. A. Thomas, *Elements of Information Theory,* 2nd Edition. New York, USA: Wiley, 2006.

[17] J. A. Thomas, "Feedback can at most double Gaussian multiple access channel capacity," *IEEE Trans. Inf. Theory*, vol. 33, no. 5, pp. 711–716, 1987.

[18] R. Rajashekar, K. V. S. Hari, and L. Hanzo, "Reduced-complexity ML detection and capacity-optimized training for spatial modulation systems," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 112-125, Jan. 2014.

[19] C. Xiao and Y. R. Zheng, "On the mutual information and power allocation for vector Gaussian channelswith finite discrete inputs," *in Proc. IEEE Global Commun. Conf. (GLOBECOM)*, New Orleans, LA, 2008.