Secrecy Capacity of Space Keying with Two Antennas

Secrecy Capacity of Space Keying with Two Antennas

Sinan Sinanovic*, Nikola Serafimovski*, Marco Di Renzo† and Harald Haas*

*Institute for Digital Communications
Joint Research Institute for Signal and Image Processing
School of Engineering
The University of Edinburgh
EH9 3JL, Edinburgh, UK
{s.sinanovic, h.haas}@ed.ac.uk

†French National Centre for Scientific Research (CNRS)
Laboratory for Signals and Systems (LSS)
École Supérieure d'Électricité (SUPELEC)
3 rue Joliot-Curie, 91192 Gif-sur-Yvette (Paris), France
marco.direnzo@lss.supelec.fr

***Abstract*—Spatial modulation (SM) and space shift keying (SSK) use only *one* out of several transmit antennas *at a time* to transmit data via an antenna index. In such a system, the information is encoded by exploiting channel randomness *i.e.* the fact that channels between different transmit and receive antennas are random. This difference is used to distinguish among the transmit antennas. While SSK uses only antenna index to transmit data, SM also uses ordinary signal modulation. In wireless secrecy systems, one of the key performance measures is secrecy capacity. It specifies the rate at which the transmitter can communicates on the main link to the desired receiver while this information cannot be decoded by the eavesdropper. We investigate SM and SSK in the context of wireless secrecy capacity when the underlying modulation and the difference between the legitimate and eavesdropper signal to noise ratios (SNRs) are varied.**

I. Introduction

A novel multiple transmitting antenna system, termed spatial modulation (SM), has been developed in [1]. The key concept is that *only one* of several transmit antennas is active at any one time. This approach is used to convey information. For example, in the case of four transmit antennas, the fact that a specific antenna is active carries two bits, in addition to the bits transmitted by the signal itself. While the rate of this system increases only logarithmically with the number of transmit antennas, its simplicity offers an interesting complexity–rate tradeoff. In [2], the SM optimum detector has been developed. A special case, termed spatial shift keying (SSK) where *only* antenna indices are used to transmit bits, has been studied in [3].

In this paper, we study SM and SSK systems in the context of secure wireless communications. The basic setting in physical layer security in wireless systems can be described as follows. In the main link, the transmitter communicates to the intended receiver, while the eavesdropper tries to decode this information. One of the important goals is to determine the rate at which the main link can be used in such a way that the eavesdropper cannot successfully decode the same information. In classical secrecy communication, a Gaussian wiretap channel has been studied where secrecy capacity is shown to be the difference between the main and eavesdropper channel capacities when the former is greater than the latter and zero otherwise [4, 5].

In recent years, multiple-input multiple-output systems [6–8] and the effects of fading [9] on secrecy capacity have been studied. In this paper, we focus on how randomness, due to the fading of the wireless channel, can help distinguish among different transmit antennas in the context of secrecy capacity. The part of the data bits which is transmitted via the antenna index is called the spatial component of the capacity of SM. This spatial components of the capacity of SM and the capacity of SSK are studied in the context of secure communication. This concept of using a specific transmit antenna and detection of its index at the receiver in order to transmit data is termed *spatial keying*. In SM case, it offers higher rate than the SISO system with the same signal constellation size. Spatial keying also has lower rate but also less complexity than the usual multiple transmit antenna techniques which require antenna synchronisation and complex receiver for decoding the parallel streams which interfere with each other.

The paper is organised as follows. In Section II, we briefly explain spatial encoding of the data. Section III explains spatial detection. In Section IV, we review symmetric channel capacity results. Section V introduces wireless secrecy concepts. In Section VII, we provide simulation results. Finally, Section VIII summarises key findings and concludes the paper with suggestions for future work.

II. Spatial Encoding of Data

A. Spatial Modulation

SM uses only one out of several transmit antennas (per channel use) to convey information in two different ways. Part of the transmitted message is encoded in the antenna number. In other words, the fact that a specific antenna is active is utilised to transmit bits. This idea relies on the ability of the receiver to distinguish between the antennas since the randomness of wireless channels associated with each transmit-receive antenna pair generally provides different channels. In simulations, it is assumed that channel coefficients are Rayleigh distributed. The remaining part of the message is encoded in a usual manner, via the signal constellation. Bits encoded in the antenna index form the *spatial symbol* while conventional modulation bits form the *radiated symbol*.

The SM system model has N_{T} transmit and N_{R} receive antennas. The underlying signal constellation is of size M.

Since $\log_2(M)$ bits are transmitted via conventional modulation and $\log_2(N_{\rm T})$ bits are transmitted via the antenna index, then one channel use corresponds to $\log_2(N_{\rm T})+\log_2(M)$ total transmitted bits. A sequence of data bits of length $\log_2(N_{\rm T})+\log_2(M)$ is mapped to a vector $\mathbf{x}$ of length $N_{\rm T}$ which is to be transmitted. Vector $\mathbf{x}$ satisfies the unity power constraint: $\mathrm{E}[\mathbf{x}^H\mathbf{x}]=1$. The channel is represented with the matrix $\mathbf{H}$ of size $N_{\rm R}$ by $N_{\rm T}$, while the noise is expressed as a vector $\mathbf{n}$ of length $N_{\rm R}$. $\mathbf{H}$ and $\mathbf{n}$ contain independent and identically distributed components with zero mean, unity variance complex Gaussian distribution, $\mathcal{CN}(0,1)$. The received signal $\mathbf{y}$ can then be written as $\mathbf{y}=\sqrt{\gamma}\mathbf{H}\mathbf{x}+\mathbf{n}$, where γ is the average received signal-to-noise ratio (SNR) at each receiving antenna. When vector $\mathbf{x}$ specifies activated antenna at position i from which the $m^{\rm th}$ constellation symbol is sent, it is denoted as $\mathbf{x}_{im}$ and the constellation symbol is denoted by x_m. Therefore, the received signal can be written as $\mathbf{y}=\sqrt{\gamma}\mathbf{h}_i x_m+\mathbf{n}$ where $\mathbf{h}_i$ denotes the $i^{\rm th}$ column of $\mathbf{H}$.

B. Space Shift Keying

One can view SSK as a special case of SM since there are no bits transmitted via the conventional modulation symbol x_m but only via the antenna index i since $x_m=1$ always holds. Equivalently, the fact that the only non-zero entry in vector $\mathbf{x}$ is at the $i^{\rm th}$ position is used to transmit information. Notation $\mathbf{x}_i$ is used to denote $i^{\rm th}$ active antenna. The received signal $\mathbf{y}$ can initially be expressed as $\mathbf{y}=\sqrt{\gamma}\mathbf{H}\mathbf{x}+\mathbf{n}$. The received signal can be more succinctly written as $\mathbf{y}=\sqrt{\gamma}\mathbf{h}_i+\mathbf{n}$. In other words, the transmitted symbol determines which column of $\mathbf{H}$ is used. SSK relies on a unique channel which can be recognised at the receiver in order to decode the information bits. One can therefore view the columns of $\mathbf{H}$ as random constellation points of SSK modulation. For example, if two antennas are available at the transmitter, activating either antenna can transmit one bit.

We note that *generalised* SSK and SM have been developed in [10, 11] where more than one antenna can be active and where antenna locations are still used to encode the data but this approach is outside of the scope of the current work.

III. Spatial Detection

A. Optimal SM Detection

The maximum likelihood (ML) detector for SM jointly detects the antenna index $\hat{i}$ and conventional modulation symbol $\hat{m}$ in the following manner [2]:

$$\begin{aligned}[\hat{i},\hat{m}] &= \arg\max_{i,m} p_{\mathbf{Y}}(\mathbf{y}|\mathbf{x}_{im},\mathbf{H}) \\ &= \arg\min_{i,m} \sqrt{\gamma}||\mathbf{g}_{im}||_{\rm F}^2 - 2{\rm Re}\{\mathbf{y}^{\rm H}\mathbf{g}_{im}\}\end{aligned}$$

where $||\cdot||_{\rm F}$ denotes the Frobenius norm, $\mathbf{g}_{im}=\mathbf{h}_i x_m$, $1\le i\le N_{\rm T}$, $1\le m\le M$ and $p_{\mathbf{Y}}(\mathbf{y}|\mathbf{x}_{im},\mathbf{H})=\pi^{-N_{\rm R}}\exp\left(-||\mathbf{y}-\sqrt{\rho}\mathbf{H}\mathbf{x}_{im}||_{\rm F}^2\right)$ is the probability density function (pdf) of $\mathbf{y}$ conditioned on $\mathbf{x}_{im}$ and $\mathbf{H}$. Knowledge of the channel $\mathbf{H}$ can be acquired by transmitting the known training sequence since the channel is assumed to be quasi-static, as in [9]. On the one hand, there is no closed form solution for the error performance of ML detector in SM [12]. The union bound approach provides a relatively tight upper bound but only for relatively large SNRs [12]. On the other hand, simulation will be used to compute the error probability of antenna detection, which is denoted by $p_{\rm SM}$. This error can then be used in conjunction with results from Section IV to ascertain the capacity of the spatial component of SM.

B. Optimal SSK Detection

The ML detector for SSK detects the antenna index $\hat{i}$ used at the transmitter in a manner similar to SM [3]:

$$\begin{aligned}\hat{i} &= \arg\max_{i} p_{\mathbf{Y}}(\mathbf{y}|\mathbf{x}_i,\mathbf{H}) \\ &= \arg\min_{i} \sqrt{\gamma}||\mathbf{h}_i||_{\rm F}^2 - 2{\rm Re}\{\mathbf{y}^{\rm H}\mathbf{h}_i\}\end{aligned}$$

where $p_{\mathbf{Y}}(\mathbf{y}|\mathbf{x}_i,\mathbf{H})=\pi^{-N_{\rm R}}\exp\left(-||\mathbf{y}-\sqrt{\rho}\mathbf{H}\mathbf{x}_i||_{\rm F}^2\right)$ is the pdf of $\mathbf{y}$ conditioned on $\mathbf{x}_i$ and $\mathbf{H}$.

As in SM case, there is no known closed form solution for the error performance of ML detector in SSK setting and the union bound approach provides relatively tight upper bound only for large SNRs [3, 13]. Simulations are therefore used to compute the error probability of antenna detection, denoted by $p_{\rm SSK}$. However, in a simple case when $N_{\rm T}=2$ and $N_{\rm R}=1$, $p_{\rm SSK}$ is known in closed form [14]:

$$p_{\rm SSK}=\frac{1}{2}\left(1-\sqrt{\frac{\gamma}{2+\gamma}}\right). \tag{1}$$

IV. Symmetric Channel

In a binary symmetric channel (BSC), there are two inputs which are correctly received at the output with probability $1-p$ and incorrectly with probability p. The capacity of this channel is

$$C_{\rm BSC}=1-H(p)\text{ bits per channel use,} \tag{2}$$

where $H(p)$ denotes the binary entropy function: $H(p)=-p\log_2(p)-(1-p)\log_2(1-p)$, [15]. The capacity is achieved for equally likely inputs. We can use the BSC approach to evaluate the capacity of the spatial component of SM and the SSK capacity with two transmitting antennas by noting that their error probabilities of antenna detection, $p_{\rm SM}$ and $p_{\rm SSK}$, can replace p in the BSC in (2). In particular, the capacity of the spatial component of SM in the case of $N_{\rm T}=2$ can be expressed as

$$C_{\rm SM}=1-H(p_{\rm SM}), \tag{3}$$

while the capacity of the SSK when $N_{\rm T}=2$ can be expressed as

$$C_{\rm SSK}=1-H(p_{\rm SSK}). \tag{4}$$

More generally, let us consider the transmission matrix where the $w^{\rm th}$ row and the $z^{\rm th}$ column denote the conditional probability $p(z|w)$ such that z is received when w is sent. Then, if the rows of the channel transition matrix are permutations of each other and the columns are permutations of each other, the channel is called *symmetric* and its capacity is given as

$$C_{\rm SYM}=\log_2|\mathcal{Z}|-H(\text{row of transition matrix}). \tag{5}$$

where the cardinality of the output set $\mathcal{Z}$ is denoted as $|\mathcal{Z}|$. The entropy $H(W)$ of a discrete random variable W with alphabet $\mathcal{W}$ is defined as $H(W) = -\sum_{w\in\mathcal{W}} p(w)\log_2(p(w))$ where the probability mass function $p(w) = \Pr\{W = w\}$. The symmetric channel can be used to evaluate the capacity of the spatial component of SM by using the fact that $|\mathcal{Z}| = N_{\mathrm{T}}$, assuming that the channels from different transmit antennas are identically distributed and noting that the row of the transition matrix has one entry. This entry denotes the probability of correctly detecting the transmit antenna, equal to $1-p_{\mathrm{SM}}$ and all other equal to $p_{\mathrm{SM}}/(N_{\mathrm{T}}-1)$, given that the confusion between any two antennas is assumed to be equally likely. Similarly, the SSK capacity can be computed by having one entry of the row of the transition matrix equal to $1-p_{\mathrm{SSK}}$ and the rest equal to $p_{\mathrm{SSK}}/(N_{\mathrm{T}}-1)$ by assuming again that the confusion between any two antennas is equally likely.

V. Wireless Secrecy Model

A. Model

In order to study secrecy capacity, we consider a situation where a user Alice transmits a message to the legitimate receiver Bob on the legitimate channel (L). The third party Eve, who is able to eavesdrop Alice's signals, is also present and its channel is denoted by subscript (E), as shown in Fig. 1. The message is communicated via $\mathbf{x}$ over a quasi-static Rayleigh fading channel on the legitimate channel

$$\mathbf{y}_L = \sqrt{\gamma_L}\mathbf{H}_L\mathbf{x} + \mathbf{n}_L \tag{6}$$

where $\mathbf{y}_L$ denotes received signal at the intended receiver, γ_L denotes SNR at the legitimate receiver, $\mathbf{H}_L$ denotes the fading coefficients and $\mathbf{n}_L$ denotes circularly symmetric complex Gaussian noise. Knowledge of the channel $\mathbf{H}_L$ can be acquired by transmitting the known training sequence. Eve receives the signal as

$$\mathbf{y}_E = \sqrt{\gamma_E}\mathbf{H}_E\mathbf{x} + \mathbf{n}_E \tag{7}$$

where $\mathbf{y}_E$ denotes the received signal at the eavesdropper, γ_E denotes SNR at the eavesdropper, $\mathbf{H}_E$ denotes the independently faded coefficients and $\mathbf{n}_E$ denotes circularly symmetric complex Gaussian noise. It is assumed that Eve knows its quasi-static channel since it will be used repeatedly.

VI. Secrecy Capacity

In this section, secrecy capacity of SSK and the spatial component of SM are characterised in a semi-analytical fashion. First, we state the secrecy capacity of the BSC. This result is then applied to SSK and SM by using the antenna detection error probabilities, which are obtained via simulation, in the expressions for the secrecy capacity of the BSC.

A. Secrecy Capacity of BSC

The secrecy capacity can be described as the maximum rate at which Alice can send information on the legitimate channel to Bob such that the rate at which eavesdropper Eve receives this information is arbitrarily small. Secrecy capacity therefore quantifies the number of bits which can be sent from Alice to Bob in secret. Let us consider BSC between Alice and Bob

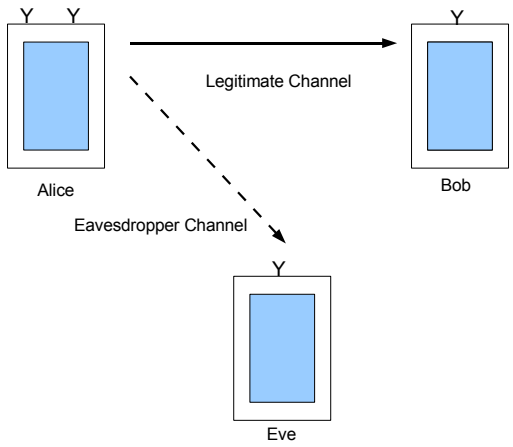

Fig. 1. Secrecy model showing legitimate user Alice with two transmit antennas and legitimate receiver Bob and eavesdropper Eve with one receiving antenna.

with the crossover probability(*i.e.* error probability) p_L and the BSC between Alice and Eve with the crossover probability p_E. It is assumed that the two BSCs are independent. Without loss of generality, it can be assumed that $p_L \leq 1/2$ and $p_E \leq 1/2$. We can now express the secrecy capacity of BSC as follows [5, 16]

$$C_s(p_L, p_E) = \begin{cases} H(p_E) - H(p_L) & \text{if } p_E > p_L, \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

In other words, non-zero secrecy capacity is only possible if the crossover probability on the channel between Alice and Eve is higher than the crossover probability on the channel between Alice and Bob. We note that the secrecy capacity can also be expressed as the difference of two BSC capacities, see (8), with crossover probabilities equal to p_L and p_E. Existence of the feedback channel changes the secrecy capacity result significantly, as shown in [17], but this is outside of the scope of this paper.

B. Secrecy Capacities of SSK and Spatial Component of SM

Let $p_{L,\mathrm{SM}}$ and $p_{E,\mathrm{SM}}$ denote error probabilities of antenna detection at the legitimate receiver and eavesdropper in the SM context. Based on (8), in the case of two transmit antennas, the secrecy capacity of the spatial component of SM can be written as

$$C_{s,\mathrm{SM}}(p_{L,\mathrm{SM}}, p_{E,\mathrm{SM}}) = H(p_{E,\mathrm{SM}}) - H(p_{L,\mathrm{SM}}) \tag{9}$$

if $p_{E,\mathrm{SM}} > p_{L,\mathrm{SM}}$. Otherwise, secrecy capacity of the spatial component of SM is equal to 0. The secrecy capacity of SSK can be expressed as

$$C_{s,\mathrm{SSK}}(p_{L,\mathrm{SSK}}, p_{E,\mathrm{SSK}}) = H(p_{E,\mathrm{SSK}}) - H(p_{L,\mathrm{SSK}}) \tag{10}$$

if $p_{E,\mathrm{SSK}} > p_{L,\mathrm{SSK}}$. Otherwise, the SSK secrecy capacity is equal to 0.

VII. Simulation Results

In this section, we quantify secrecy capacities of the spatial component of SM and SSK by employing the semi-analytical approach. Simulations of communication with optimal SM

and SSK detectors are performed in order to obtain their respective error probabilities of antenna detection, p_{SM} and p_{SSK} for different values of SNR since union bound values for error probability are precise only for high SNR. The SNR value is varied at the legitimate receiver to obtain a range of error probabilities of antenna detection $p_{L,\mathrm{SM}}$ and $p_{L,\mathrm{SSK}}$ while the eavesdropper's SNR is kept fixed to provide corresponding $p_{E,\mathrm{SM}}$ and $p_{E,\mathrm{SSK}}$. The secrecy capacity of the spatial component of SM is computed by using (9) and the secrecy capacity of SSK by using (10). The results are plotted to show secrecy capacity versus SNR on the legitimate channel while SNR at the eavesdropper is kept at some fixed value for a particular scenario.

We first start by plotting error probabilities of antenna detection in SSK and SM for a varying size of the signal constellation M for a system with $N_{\mathrm{T}}{=}2$ and $N_{\mathrm{R}}{=}1$ in Fig. 2. For $M = 2$, binary phase shift keying (BPSK) is used, while for the other values of M quadrature amplitude (QAM) modulation is employed. We first note that the SSK theoretical

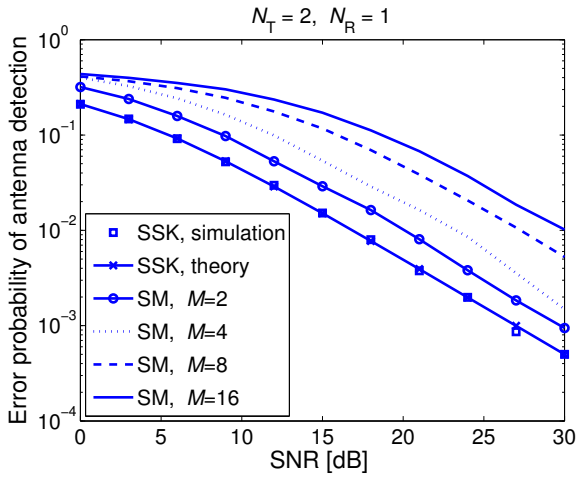

Fig. 2. Comparison of error probabilities of antenna detection in SSK and SM with underlying signal constellations of different sizes.

result in (1) agrees with the simulation. As expected, SSK has the best error performance since the receiver only has to detect the antenna index as opposed to SM where both the antenna index *and* the underlying signal constellation symbol have to be detected. Furthermore, as the size of the constellation increases, the error performance predictably worsens since the constellation points move closer to each other. We also note that, for larger SNR values, the slopes of the error curves are the same: they are equal to -1 since a tenfold decrease of error corresponds to an SNR increase of 10 dB when $N_{\mathrm{R}}{=}1$. The gap between the error curves is due to the difference in the underlying constellation sizes: as constellations grow, the necessary SNR to achieve the same error probability also grows. Based on the fact that SSK has superior error performance over the spatial component of SM for all constellation sizes, *i.e.* $p_{\mathrm{SSK}}{<}p_{\mathrm{SM}}$ at a given SNR, one might suspect that SSK would have better secrecy capacity than SM. We show next, however, that this is not necessarily the case.

We start the characterisation of the secrecy capacity by considering the case of $N_{\mathrm{T}}{=}2$ and $N_{\mathrm{R}}{=}1$ with SNR at the eavesdropper being fixed at 0 dB, while the SNR at the legitimate link varies, as shown in Fig. 3. SM secrecy capacity

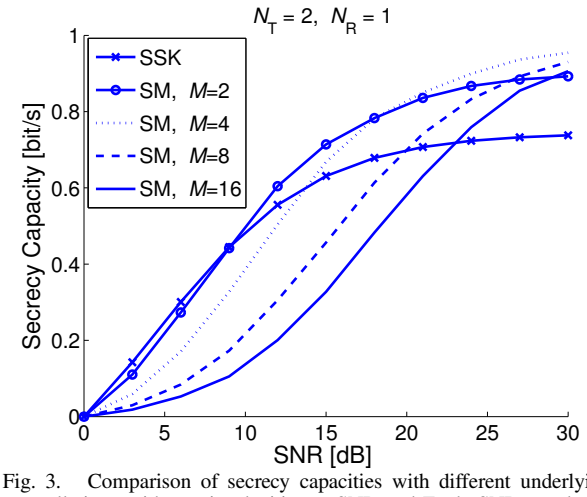

Fig. 3. Comparison of secrecy capacities with different underlying signal constellations with varying legitimate SNR and Eve's SNR equal to 0 dB.

decreases, except for high SNRs, as the constellation size increases. While SSK provides larger secrecy capacity than the SM variants at lower SNRs, SM secrecy capacities for all M overtake SSK secrecy capacity for sufficiently high SNRs. This, somewhat counterintuitive, result can be understood by considering the secrecy capacity as the SNR on the legitimate link increases to infinity. It is easily seen that p_L tends to zero as SNR on the legitimate link goes to infinity. Since the BSC secrecy capacity is expressed as the difference of two binary entropies evaluated at p_E and p_L, as in (8), we have that $C_s(0, p_E){=}H(p_E)$ in the limit. In the case of SSK, secrecy capacity is asymptotically given by

$$C_{s,\mathrm{SSK}}(0, p_{E,\mathrm{SSK}}){=}H(p_{E,\mathrm{SSK}}), \tag{11}$$

while in the case of SM, it is

$$C_{s,\mathrm{SM}}(0, p_{E,\mathrm{SM}}){=}H(p_{E,\mathrm{SM}}). \tag{12}$$

Since, as discussed earlier, $p_{E,\mathrm{SM}}{>}p_{E,\mathrm{SSK}}$, it follows that $H(p_{E,\mathrm{SM}}){>}H(p_{E,\mathrm{SSK}})$ because the binary entropy is an increasing function for crossover probabilities less than a half. Therefore, it becomes clear that, as the SNR on the legitimate channel tends to infinity, secrecy capacity of the spatial component of SM becomes larger than the SSK secrecy capacity. Paradoxically, the main reason for SM outperforming SSK in terms of secrecy capacity is that SM *underperforms* in terms of the error probability of antenna detection. This phenomenon also explains why, for a large SNR, SM performs better for large M than for small M.

We next study the changes in secrecy capacity when Eve's SNR is equal to 12 dB. Fig. 4 shows that secrecy capacities are lower than the counterparts in Fig. 3. Naturally, the secrecy capacity is equal to zero when the legitimate receiver's SNR is below 12 dB. At higher SNRs, it can be seen that SM with the highest M, $M{=}16$, outperforms other schemes. This is due to the asymptotic behaviour of the secrecy capacity when SNR tends to infinity, as discussed earlier in the section.

Finally, we observe the changes in the secrecy capacity when Eve's SNR is equal to 21 dB. Fig. 5 shows that the

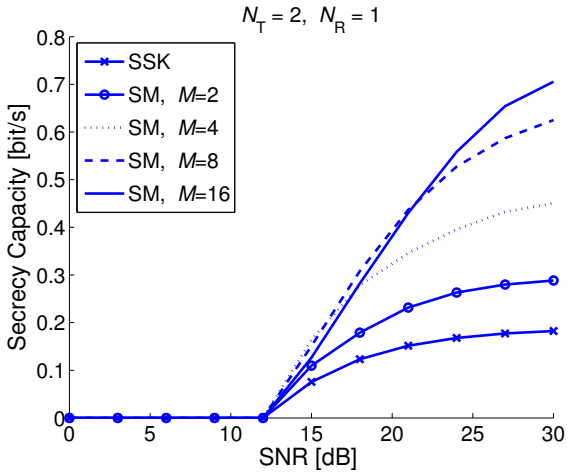

Fig. 4. Comparison of secrecy capacities with different underlying signal constellations with varying legitimate SNR and Eve's SNR equal to 12 dB.

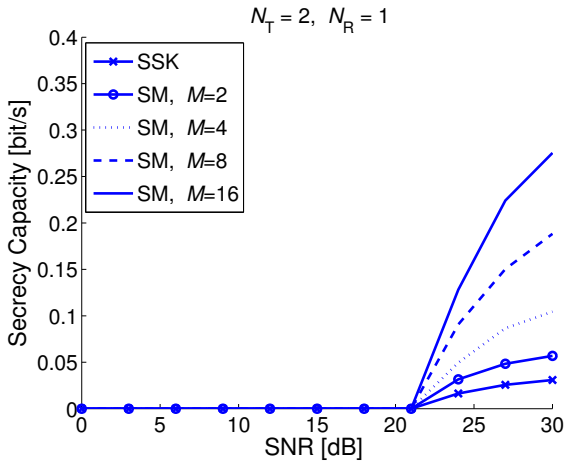

Fig. 5. Comparison of secrecy capacities with different underlying signal constellations with varying legitimate SNR and Eve's SNR equal to 21 dB.

secrecy capacities are even lower than the corresponding values in Fig. 3 and 4. This is to be expected since the gap between Bob's and Eve's SNRs is smaller and, consequently, the difference between their capacities is also smaller. At high SNRs, the advantage of larger M becomes even more apparent in this case compared to the previous two cases shown in Fig. 3 and 4.

VIII. Summary and Conclusions

We have explored secrecy capacity of the spatial component of SM and SSK systems. We have shown that the effect of constellation size depends on the values of the legitimate and eavesdropper's SNRs. For low eavesdropper's SNR, smaller constellations perform better than larger ones for most of the SNR range, while for the high eavesdropper's SNR, larger constellations provide larger secrecy capacities. As the gap between the eavesdropper's and legitimate receiver's SNRs is reduced, the secrecy capacity is significantly reduced for SM and SSK. Furthermore, while SSK secrecy capacity may be expected to perform better due to the lack of conventional modulation and its smaller error of antenna detection, it actually performs worse than the secrecy capacity of the spatial component of SM at high SNR precisely due to the smaller error probability. Future work will seek to tighten probability of error obtained via union bound so that it can be used for fully analytical computation of SM and SSK capacity. Furthermore, effects of varying the number of transmit and receive antennas on secrecy capacity will be explored.

Acknowledgment

Professor Haas acknowledges the Scottish Funding Council support of his position within the Edinburgh Research Partnership in Engineering and Mathematics between the University of Edinburgh and Heriot Watt University. We gratefully acknowledge support from the Engineering and Physical Sciences Research Council (EP/G011788/1) in the United Kingdom for this work.

References

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

[2] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Spatial Modulation: Optimal Detection and Performance Analysis," *IEEE Commun. Lett.*, vol. 12, no. 8, pp. 545–547, 2008.

[3] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space Shift Keying Modulation for MIMO Channels," *IEEE Transaction on Wireless Communications*, vol. 8, no. 7, pp. 3692–3703, Jul. 2009.

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

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[6] 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.

[7] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," in *IEEE International Symposium on Information Theory*, Toronto, ON, 2008, pp. 524–528.

[8] Z. Li, W. Trappe, and R. Yates, "Secret Communication Via Multi-Antenna Transmission," in *41st Annual Conference on Information Sciences and Systems, CISS '07.*, Baltimore, MD, 2007, pp. 905–910.

[9] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," in *IEEE International Symposium on Information Theory*, Seattle, WA, 2006, pp. 356–360.

[10] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proc. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC 2008*, Cannes, France, 15–18 September 2008, pp. 1–5.

[11] A. Younis, N. Serafimovski, R. Mesleh, and H. Haas, "Generalized Spatial Modulation," in *Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, 2010.

[12] M. Di Renzo and H. Haas, "Performance analysis of spatial modulation," in *5th International ICST Conference on Communications and Networking in China*, August 2010.

[13] ——, "Performance Analysis of Spatial Modulation," in *IEEE International Conference on Communication and Networking in China (CHINACOM)*, Beijing, China, Aug. 2010, pp. 1–7, (invited paper).

[14] ——, "Performance Comparison of Different Spatial Modulation Schemes in Correlated Fading Channels," in *Proc. of International Conference on Communications*, May 2010.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 1st ed., ser. Wiley Series in Telecommunications, D. L. Schilling, Ed. John Wiley & Sons, Sep. 1991.

[16] U. M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[17] L. Lai, H. Elgamal, and V. Poor, "The Wiretap Channel With Feedback: Encryption Over the Channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 5059–5067, 2008.