Secure Space Shift Keying Transmission Using Dynamic Antenna Index Assignment

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

***Abstract*—We propose a secure transmission scheme based on space shift keying (SSK) in which the indices associated with the transmit antennas are assigned dynamically according to the channel towards the legitimate receiver. We first derive an asymptotic secrecy rate under the perfect channel reciprocity assumption. Then, we study the impacts of imperfect reciprocity and presence of a nearby eavesdropper on the reliability and eavesdropping resilience of the proposed scheme. Finally, we introduce an enhanced antenna index assignment algorithm which is more robust to imperfect reciprocity, and is capable of preventing a nearby eavesdropper from acquiring the transmitted bits.**

Index Terms — Physical layer security, MIMO wiretap channel, space shift keying.

I. Introduction

Security is one of the major concerns in wireless communications. Recently, there has been a considerable growth of interest in studying the capabilities of the physical layer in providing secrecy. In [1], Wyner demonstrated the possibility of realizing secure communications in the absence of a secret key. Extensive recent studies have investigated information-theoretic limits of secure communications for several important scenarios including fading channels [2] and multiple-input multiple-output multiple-antenna-eavesdropper (MIMOME) wiretap channels [3]-[5].

In addition to the investigation of information-theoretic limits of secure communications over different channels, a recent major focus has been on proposing practical approaches to secure wireless transmission at the physical layer. A common feature of many of these schemes is to exploit the user-dependent randomness introduced by the wireless channel for secrecy extraction. The fact that the physical channel between the legitimate users is inaccessible for an eavesdropper who is at a distance larger than half a wavelength from the legitimate receiver, allows the legitimate users to employ the channel state information (CSI) as their shared secrecy. For instance, the authors in [6] take advantage of the CSI shared between transmitter and legitimate receiver to interleave the subcarriers of the OFDM signals according to a decreasing order of their instantaneous channel gains. With the proposed transmission scheme, an eavesdropper, who is unable to obtain the de-interleaving pattern, fails to detect the transmitted bits.

Space shift keying (SSK) is a relatively new MIMO transmission scheme which relies on embedding information onto the active antenna indices [7]. Along with the various studies which explore different potential applications of SSK [8], several recent articles have studied its use over MIMO wiretap channels. An initial study of SSK transmission in the context of physical layer security is reported in [9] where an achievable secrecy rate is derived and characterized for different number of transmit and receive antennas. Various secure SSK transmission schemes have also been proposed, which rely on precoding [10]-[12] or artificial noise injection [13]-[14].

In this work, we propose a new secure transmission scheme which relies on SSK with dynamic antenna index assignment. In particular, we adopt an antenna index assignment scheme which varies from one block of information bits to another according to the channel between the legitimate users. The transmitter assigns the antenna indices according to a decreasing order of the magnitudes of their instantaneous channel gains. If the channel reciprocity holds, the legitimate receiver can simply acquire the antenna index assignment pattern initiated by the transmitter and can detect the transmitted bits accordingly. In contrast, an eavesdropper which is sufficiently far from the legitimate receiver observing a statistically independent channel cannot track the antenna index assignment pattern, and as a result, it fails to detect the message.

In this paper, we first evaluate the achievable secrecy rates for the scenarios with perfect channel reciprocity and an eavesdropper with an independent channel for high signal-to-noise ratios (SNRs). We also study the impacts of imperfect reciprocity and presence of a nearby eavesdropper. The imperfect reciprocity results in a mismatched antenna index assignment pattern at the legitimate users and deteriorates the reliability of transmission. Moreover, an eavesdropper who is sufficiently close to the legitimate receiver may observe a channel that is correlated with that of the legitimate receiver. In presence of such an eavesdropper the security of the proposed scheme is breached.

So as to resolve the above-mentioned deficiencies, we also propose a practical secure transmission scheme in which antenna index assignment is carried out according to a rotated legitimate channel. Inspired by the channel estimation scheme proposed in [15], we include a training session which is done with reference signals rotated by random unitary matrices selected from a codebook, which is assumed to be known by all the parties including the eavesdropper. The advantages of

978-1-5090-5019-2/17/$31.00 ©2017 IEEE

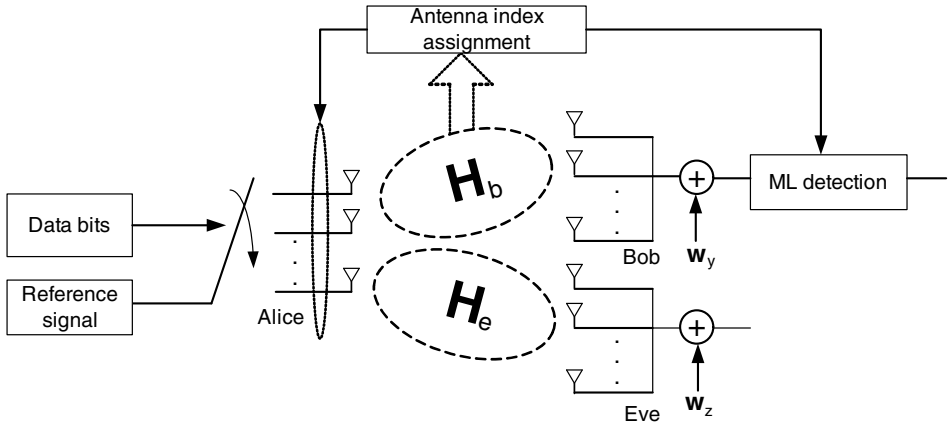

Fig. 1: The system model.

this approach are two-fold: First, since the specific unitary matrices utilized are only known by the legitimate users, the eavesdropper is unable to acquire the antenna index assignment even if her channel is highly correlated with the legitimate user's channel. The second advantage is that, by selecting the unitary matrix from the codebook in a manner that the minimum channel magnitude difference among the antennas is maximized, the probability of mismatched antenna index assignment pattern at the legitimate users is reduced, and accordingly, we can improve the reliability for the scenarios with imperfect reciprocity.

The paper is organized as follows. The system model is described in Section II. In Sections III and IV, we propose two secure transmission schemes based on SSK with dynamic antenna index assignment. The performance of the proposed schemes is evaluated using numerical experiments and the results are reported in Section V. Section VI concludes the paper.

II. System Model

Consider a general MIMOME wiretap channel as depicted in Fig. 1. The transmitter, Alice, the legitimate receiver, Bob, and the eavesdropper, Eve, are assumed to be equipped with N_t, N_{r_b} and N_{r_e} antennas, respectively. We consider the use of SSK for which the antenna indices are employed for embedding user data, therefore a one-to-one mapping is established between the blocks of information bits to be transmitted and the indices of the transmit antennas in the array [7].

The received signals at the legitimate receiver and the eavesdropper are given by

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

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

where $\mathbf{H}_b$ and $\mathbf{H}_e$ are the $N_{r_b} \times N_t$ and $N_{r_e} \times N_t$ channel matrices corresponding to the legitimate channel and the eavesdropper's channel, respectively. The elements of the channel matrices are independent and identically distributed (i.i.d.) zero-mean and unit-variance circularly symmetric complex Gaussian random variables $\mathcal{CN}(0,1)$. We consider a block fading scenario in which $\mathbf{H}_b$ and $\mathbf{H}_e$ remain constant over a block of N_c symbols and vary independently from one block to the next. The transmitted symbol, $\mathbf{x}$, is of the form $[0\ 0\ ...\ 1\ ...\ 0]^T$, with the position of 1 indicating the antenna being activated. In (1) and (2), $\mathbf{w}_y$ and $\mathbf{w}_z$ are additive white Gaussian noise vectors which follow $\mathcal{CN}(0,\sigma_b^2)$ and $\mathcal{CN}(0,\sigma_e^2)$, respectively. Furthermore, $\mathbf{H}_b$, $\mathbf{H}_e$, $\mathbf{w}_y$ and $\mathbf{w}_z$ are independent. We assume that the fading process is ergodic. We also assume that the response of the channel from the transmitter to the legitimate receiver is identical to the response in the opposite direction. The legitimate receiver and the eavesdropper estimate their own channels perfectly. However, the transmitter may estimate the main channel correctly or erroneously depending on whether the reciprocity is perfect or imperfect.

III. CSI-based Antenna Index Assignment

In this section, we propose an SSK transmission scheme which provides communication confidentiality via not allowing the eavesdropper to determine the indices of antennas activated. In order to realize such a transmission scheme, the transmitter and the legitimate receiver obtain local channel estimates. This is to say, training signals are transmitted from the transmitter to the legitimate receiver and vice versa as depicted in Fig. 2. We refer to this scheme as Scheme 1. After estimating the channel, the transmitter sorts the columns of the channel matrix and assigns indices to the antennas in such a way that $\|\mathbf{h}_{b_1}\|^2 \geq \|\mathbf{h}_{b_2}\|^2 \geq \ldots \geq \|\mathbf{h}_{b_{N_t}}\|^2$. Based on channel reciprocity, the legitimate receiver can obtain the antenna index assignment pattern initiated by the transmitter through its local channel estimate, and then decode the transmitted message. In contrast, the eavesdropper receiving the signal through a statistically independent channel cannot track the antenna index assignment pattern, and as a result, fails to detect the message.

A. Asymptotic Ergodic Secrecy Rates with Perfect Reciprocity

In this section, we perform an information-theoretic analysis of the proposed scheme under the perfect reciprocity assumption. More specifically, we derive the asymptotic secrecy rate for SSK with CSI-based antenna index assignment for high SNRs. With perfect reciprocity, the setup is equivalent to the case of a wiretap channel with the main channel CSI only, and the ergodic achievable secrecy rates are evaluated as [2]

$$R_s = \mathbb{E}_{\mathbf{H}_b,\mathbf{H}_e}\Big\{\big(I(\mathbf{x};\mathbf{y}|\mathbf{H}_b) - I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)\big)^+\Big\}, \tag{3}$$

where $I(\mathbf{x};\mathbf{y}|\mathbf{H}_b)$ and $I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)$ are mutual information terms corresponding to the main channel and the eavesdropper's channel, respectively. For an asymptotic analysis, we assume that $\sigma_b \to 0$ and $\sigma_e \to 0$. As a result, both of the receivers are capable of detecting the antennas which have been activated at the transmitter correctly. In this case, the legitimate receiver achieves the maximum rate, i.e., $\log N_t$ bits per transmission. However, the eavesdropper can only make a random guess among the $N_t!$ words of length $n_c = N_c \log N_t$ bits. Hence, the mutual information for the eavesdropper can be calculated as [16]

$$I(\hat{\mathbf{x}}^{n_c};\hat{\mathbf{z}}^{n_c}) = H(\hat{\mathbf{z}}^{n_c}) - H(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}), \tag{4}$$

where $\hat{\mathbf{x}}$ denotes the transmitted bits and $\hat{\mathbf{z}}$ denotes the received bits at the eavesdropper. The mutual information in (4) is calculated using

$$H(\hat{\mathbf{z}}^{n_c}) = n_c, \tag{5}$$

$$H(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}) = \sum_{(\hat{\mathbf{x}}^{n_c},\hat{\mathbf{z}}^{n_c})\in\mathcal{X}\times\mathcal{Z}} p(\hat{\mathbf{x}}^{n_c},\hat{\mathbf{z}}^{n_c}) \log\left(\frac{1}{p(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c})}\right), \tag{6}$$

in which,

$$p(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}) = \frac{1}{N_t!}, \tag{7}$$

$$p(\hat{\mathbf{x}}^{n_c},\hat{\mathbf{z}}^{n_c}) = p(\hat{\mathbf{x}}^{n_c})p(\hat{\mathbf{z}}^{n_c}|\hat{\mathbf{x}}^{n_c}) = \left(\frac{1}{2}\right)^{n_c}\frac{1}{N_t!}. \tag{8}$$

As a result, (4) becomes

$$I(\hat{\mathbf{x}}^{n_c};\hat{\mathbf{z}}^{n_c}) = n_c - \log(N_t!) \quad \text{(bits)}. \tag{9}$$

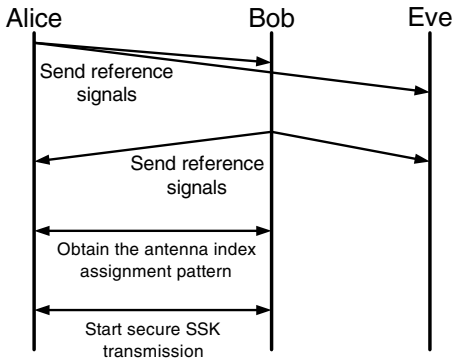

Fig. 2: CSI-based antenna index assignment (Scheme 1).

Therefore, at high SNRs, the mutual information at the eavesdropper, i.e., $I(\mathbf{x};\mathbf{z}|\mathbf{H}_e)$, approaches $\log N_t - \frac{\log(N_t!)}{N_c}$ bits per transmission and the achievable secrecy rate is given by

$$R_{s,asymp} = \frac{\log(N_t!)}{N_c} \quad \text{(bpcu)}, \tag{10}$$

where bpcu is short for bits per channel use.

B. Reliability under Imperfect Reciprocity

Channel estimation errors can result in mismatched antenna indices at the legitimate users. To model such an imperfect channel estimation at the transmitter, we assume that the estimate is a noisy version of the actual channel [17], i.e.,

$$\tilde{\mathbf{h}}_{b_i} = \sqrt{1-\tau^2}\mathbf{h}_{b_i} + \tau\mathbf{q}_i, \tag{11}$$

where $\tilde{\mathbf{h}}_{b_i}$ is the estimated channel between the i^{th} transmit antenna and the receive antennas, $\mathbf{q}_i$ is the i^{th} column of an $N_{r_b} \times N_t$ random matrix $\mathbf{Q}$ which follows $\mathcal{CN}(0,\mathbf{I})$, and τ is a parameter which determines the quality of estimation. While in the scenarios with perfect reciprocity, the symbol error probability of the proposed transmission scheme is equal to that of the conventional SSK, in the presence of the channel estimation errors at the transmitter, the mismatched antenna index assignment pattern can increase the symbol error rate (SER). More specifically, the SER of the proposed SSK with the CSI-based antenna index assignment is given by

$$P_{SER} \approx 1 - P_I(1 - P'_{SER}), \tag{12}$$

where P'_{SER} denotes the SER of the conventional SSK and P_I stands for the probability of the identical antenna indices at the legitimate users, which can be calculated as

$$P_I = P(\theta_A|\theta_B), \tag{13}$$

where θ_A and θ_B stand for the events that $\|\tilde{\mathbf{h}}_{b_1}\|^2 \geq \|\tilde{\mathbf{h}}_{b_2}\|^2 \geq \ldots \geq \|\tilde{\mathbf{h}}_{b_{N_t}}\|^2$ and $\|\mathbf{h}_{b_1}\|^2 \geq \|\mathbf{h}_{b_2}\|^2 \geq \ldots \geq \|\mathbf{h}_{b_{N_t}}\|^2$, respectively. Clearly, the quality of channel estimation plays a vital role in keeping the probability of error acceptably low. On the other hand, the channels in which the norm squares of the columns are close to each other are more prone to the occurrence of mismatched antenna indices. Consider the simple case of a MISO main channel with $N_t = 2$. Given that $|h_1|^2 \geq |h_2|^2$, the probability of having mismatched antenna indices is equal to

$$P_{MI} = 1 - P_I = P\{|\tilde{h}_1|^2 < |\tilde{h}_2|^2\} = P\{|\tilde{h}_1|^2 - |\tilde{h}_2|^2 < 0\}. \tag{14}$$

Noting that from (11), conditioned on the actual channel gains, $\tilde{h}_1$ and $\tilde{h}_2$ are distributed as $\mathcal{CN}(\sqrt{1-\tau^2}h_1, \tau^2)$ and $\mathcal{CN}(\sqrt{1-\tau^2}h_2, \tau^2)$, respectively, and $D = |\tilde{h}_1|^2 - |\tilde{h}_2|^2$ is difference of two independent chi-square random variables. Hence, conditioned on h_1 and h_2, the probability of mis-

TABLE I: Probability of antenna index mismatch for $\tau = 0.05$.

Δ \ $\lvert h_1\rvert^2$	0.25	0.5	0.75	1
0.05	0.1462	0.2344	0.2788	0.3066
0.1	0.0123	0.0681	0.1162	0.1527
0.15	0.0001	0.0106	0.0340	0.0596
0.2	0.0000	0.0007	0.0065	0.0175

matched antenna indices in (14) can be evaluated using [18, Eq. (4)] as

$$P_{MI} = Q_1\Big(\sqrt{\frac{1-\tau^2}{\tau^2}}|h_2|\ ,\ \sqrt{\frac{1-\tau^2}{\tau^2}}|h_1|\Big) - \frac{1}{2}\exp\Big(-\frac{1-\tau^2}{2\tau^2}(|h_1|^2+|h_2|^2)\Big)I_0\Big(\frac{1-\tau^2}{\tau^2}|h_1||h_2|\Big), \tag{15}$$

where $Q_1(.,.)$ is the first-order Marcum Q-function

$$Q_1(a,b) = \int_b^\infty u\exp\Big(-\frac{(u^2+a^2)}{2}\Big)I_0(au)du, \tag{16}$$

and $I_0(.,.)$ denotes the 0^{th}-order modified Bessel function of the first kind. Defining $\Delta = |h_1|^2 - |h_2|^2$, we can rewrite (15) as

$$P_{MI} = Q_1\Big(\sqrt{\frac{1-\tau^2}{\tau^2}(|h_1|^2-\Delta)}\ ,\ \sqrt{\frac{1-\tau^2}{\tau^2}}|h_1|\Big) - \frac{1}{2}\exp\Big(-\frac{1-\tau^2}{2\tau^2}(2|h_1|^2-\Delta)\Big)I_0\Big(\frac{1-\tau^2}{\tau^2}|h_1|\sqrt{|h_1|^2-\Delta}\Big). \tag{17}$$

Table I illustrates the values of P_{MI} obtained from evaluation of (17) for different values of $|h_1|^2$ and Δ. It is seen from this table that for a fixed $|h_1|^2$ and a given quality of channel estimation τ, increasing Δ can decrease the probability of antenna index mismatch at the legitimate users, as expected.

C. Threat of a Nearby Eavesdropper

Security of the SSK scheme with a CSI-based antenna index assignment relies on the spatial separation between Bob and Eve. That is, if the wireless channel experienced by Eve is similar to the one experienced by Alice and Bob, the security will easily be breached. It is well known that the channel experienced by a nearby eavesdropper may be highly correlated with the main channel [19]. Denoting the vector representation of the channel matrices $\mathbf{H}_b$ and $\mathbf{H}_e$ as

$$\mathbf{g}_b = \text{vec}(\mathbf{H}_b), \tag{18}$$

$$\mathbf{g}_e = \text{vec}(\mathbf{H}_e), \tag{19}$$

we model the correlation between $\mathbf{H}_b$ and $\mathbf{H}_e$ using [15, Eq. (31)]

$$\mathbb{E}\{\mathbf{g}_e\mathbf{g}_b^H\} = \rho\mathbf{I}, \tag{20}$$

where ρ is a parameter which takes values in the interval $[-1\ \ 1]$. When $\mathbf{H}_b$ and $\mathbf{H}_e$ are independent, we have $\rho = 0$. However, some recent experiments have shown that an eavesdropper which is sufficiently close to the legitimate receiver can experience a channel, which is correlated with the main channel with a correlation parameter as high as $\rho = 0.99$ [19], which allows the adversary to infer significant portions of the data transmitted using Scheme 1.

IV. Dynamic Antenna Index Assignment based on Rotated Channels

To remedy the problems stated in Sections III-B and III-C, in this section, we provide an antenna index assignment scheme, which is robust to imperfect reciprocity and also able to mitigate the threat of a nearby eavesdropper. The basic idea is to perform the antenna index assignment according to a rotated channel. So as to avoid wiretapping by an eavesdropper who is potentially close to the legitimate receiver or the transmitter, the rotation matrix should be kept secret. Furthermore, by selecting this rotation matrix in a manner that the magnitude squares of the channel gains are maximally separated, robustness against the channel estimation errors can be enhanced.

The procedure for the proposed dynamic antenna index assignment according to the rotated channel (referred to as Scheme 2) is illustrated in Fig. 3. In order for the legitimate users to obtain the rotated channel, the following steps are taken:

- Alice sends a reference signal to Bob which makes it possible for him to estimate the main channel, $\mathbf{H}_b$. Bob then locally generates a codebook of isotropic random unitary matrices (by applying the singular value decomposition (SVD) on zero-mean complex Gaussian matrices).
- Alice generates a secret sequence $\mathbf{s}$ and sends it to Bob.
- Bob selects a rotation matrix $\mathbf{G}$ among the matrices in the codebook which maximizes the minimum distance among the norm squares of the columns of the rotated channel. Bob then multiplies the received signal by $\mathbf{G}$ and echoes it back to Alice.

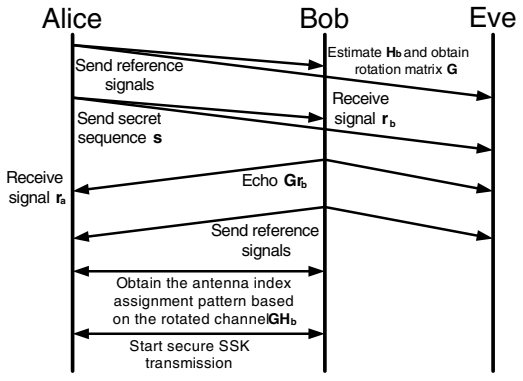

Fig. 3: Dynamic antenna index assignment to avoid wiretapping by a nearby eavesdropper (Scheme 2).

- Finally, Bob sends a reference signal to Alice which allows her to estimate the main channel, and accordingly retrieve $\mathbf{G}$.

This strategy mitigates the threat of a nearby eavesdropper. This is because the information of the secret sequence is only known by Alice, i.e., she is the only one who can acquire $\mathbf{G}$. By taking advantage of her knowledge on $\mathbf{s}$ and $\tilde{\mathbf{H}}_b$, Alice can acquire the rotated channel $\mathbf{F}_b = \mathbf{G}\mathbf{H}_b$ from the echoed signal which is given by

$$\mathbf{r}_a = \mathbf{H}_b\mathbf{F}_b\mathbf{s} + \mathbf{H}_b\mathbf{G}\mathbf{w}_1 + \mathbf{w}_2, \tag{21}$$

where $\mathbf{w}_1$ and $\mathbf{w}_2$ are additive white Gaussian noise terms at Bob (echoed back to Alice) and at Alice, respectively. Alice estimates $\mathbf{H}_b\mathbf{F}_b$ from (21) (e.g., using a least square solution) and hence she acquires the rotated channel $\mathbf{F}_b$ using her knowledge on $\mathbf{H}_b$. A nearby Eve, in contrast, cannot acquire any information about $\mathbf{G}$ and as a result, fails to detect the bits transmitted. Moreover, since Bob selects the rotation matrix using the following rule

$$\mathbf{G}_{\hat{k}} = \arg\max_{k} \min_{\forall i,j} \left| \|\mathbf{f}_{b_{ki}}\|^2 - \|\mathbf{f}_{b_{kj}}\|^2 \right| \quad i,j = 1,\ldots,N_t, \quad j \neq i, \tag{22}$$

where $\mathbf{f}_{b_{ki}}$ is the i^{th} column of the rotated channel corresponding to the k^{th} rotation matrix (i.e., $\mathbf{F}_{bk}$), the probability of a mismatched antenna index assignment between the legitimate users is reduced. The price to be paid in implementation of Scheme 2 with respect to Scheme 1 is the need for two extra steps in the process of obtaining the antenna index assignment pattern.

V. Numerical Examples

This section provides several numerical examples to demonstrate the efficacy of the proposed transmission schemes. Throughout the simulations, we assume that the main and the eavesdropper's channels follow the same statistics and the additive noise terms at both receivers have equal variances.

Fig. 4 demonstrates the asymptotic secrecy rates for the proposed SSK transmission scheme with the CSI-based antenna index assignment. It is assumed that the perfect reciprocity holds, and hence, the achievable secrecy rates for high SNRs are evaluated using (10). It can be inferred from the figure that increasing the number of transmit antennas yields considerable gains in terms of the secrecy rates. Since an eavesdropper experiencing an independent channel cannot do any better than a random guess among the $N_t!$ possible word choices, increasing the number of transmit antennas increases her confusion. Furthermore, it is clear from (10), and also from the figure, that the secrecy rates are reduced with an increased channel coherence time.

In order to compare the performance of the two proposed algorithms, we perform Monte Carlo simulations to obtain the bit error rates (BERs)[1] at Bob and Eve under perfect and imperfect CSI scenarios. We consider a MIMOME wiretap

[1]Although BER is used as a practical metric for quantifying the eavesdropping resilience, it satisfies neither the strong nor the weak secrecy constraints.

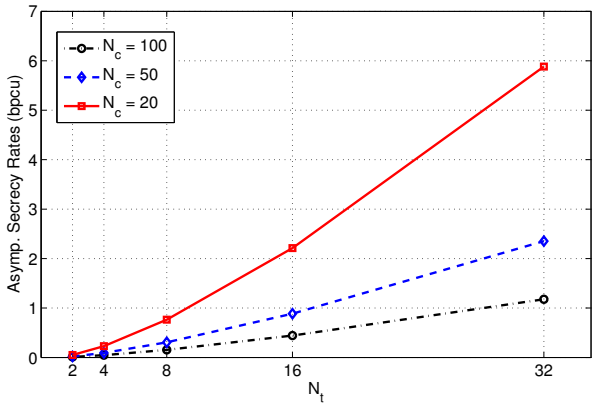

Fig. 4: Achievable secrecy rates at high SNRs for SSK transmissions with the CSI-based antenna index assignment under perfect reciprocity.

channel with $(N_t, N_{r,b}, N_{r,e}) = (4,1,1)$ employing SSK transmission. We model the imperfect CSI at Alice as follows. When employing Scheme 1, the estimated channel at Alice is given as in (11). Similarly, when Scheme 2 is employed, the estimated rotated channel at the transmitter is modeled as $\tilde{\mathbf{f}}_{b_i} = \sqrt{1-\tau^2}\mathbf{f}_{b_i} + \tau\mathbf{q}_i$. Furthermore, the correlation between the main channel and the eavesdropper's channel is modeled using (20). A rotation matrix codebook of size 100 is considered for Scheme 2. Fig. 5 compares the resulting BERs at the legitimate receiver and the eavesdropper where both receivers are assumed to employ maximum likelihood (ML) detection [7]. It is clear that the SSK scheme with the CSI-based antenna index assignment is capable of providing good reliability and eavesdropping resilience for the scenarios with perfect reciprocity ($\tau = 0$) and uncorrelated eavesdropper's channel ($\rho = 0$). However, an imperfect reciprocity (with

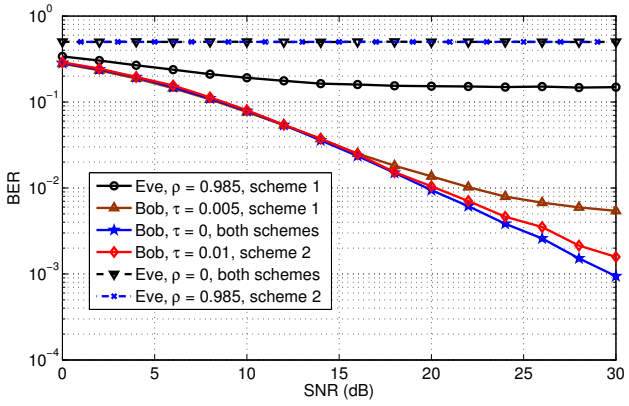

Fig. 5: BER for SSK with $N_t = 4$, $N_{r_b} = N_{r_e} = 1$ under perfect and imperfect reciprocity, and with and without channel correlation between Bob and Eve.

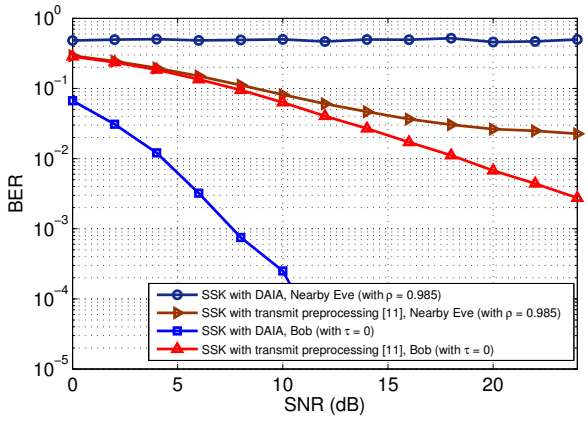

Fig. 6: SSK with dynamic antenna index assignment (DAIA) and the transmit preprocessing scheme proposed in [11], $(N_t, N_{r_b}, N_{r_e}) = (4, 4, 4)$.

$\tau = 0.005$) considerably degrades the BER at Bob, and a correlated eavesdropper (with $\rho = 0.985$) is capable of breaching the security of the system. We also observe that the second scheme, which relies on antenna index assignment according to a rotated channel is more robust to imperfect reciprocity (with $\tau = 0.01$), and also it prevents a correlated eavesdropper (with $\rho = 0.985$) from tracking the antenna index assignment pattern, correctly.

Finally, we compare the performance of the proposed dynamic antenna index assignment technique with that of the secure SSK and spatial modulation scheme proposed in [11], which relies on transmit preprocessing. In the secure transmission scheme of [11], with the assumption that the main channel is reciprocal, the channel estimation is carried out only in the reverse direction (from Bob to Alice). Then, Alice takes advantage of the estimated channel to design transmit preprocessing coefficients, which cancel the effect of fading at Bob so that he can detect the transmitted bits with no need for CSI. For the scenarios with $N_t = N_{r_b}$, these coefficients are attained by normalizing $\mathbf{H}_b^{-1}$. Fig. 6 compares the reliability and eavesdropping resilience of this technique with those of Scheme 2 proposed in Section IV. We depict the BER at Bob and at a nearby Eve (with $\rho = 0.985$) with $N_t = N_{r_b} = N_{r_e} = 4$. It can be inferred from Fig. 6 that, unlike the newly proposed scheme, the security of the one in [11] is breached in such scenarios. Moreover, since in the proposed SSK scheme with a dynamic antenna index assignment, the CSI is available at Bob, he can take advantage of the optimal ML detection. As a result, the proposed scheme yields a considerably smaller error probability at the legitimate receiver, and achieves a higher reliability.

VI. Conclusions

We have proposed an eavesdropping resilient transmission scheme using SSK with randomized antenna index assignment. Exploiting the channel between the legitimate users as a source of common randomness, two algorithms have been introduced for acquiring the indices of transmit antennas. It has been shown that the proposed antenna index assignment algorithm based on the rotated channel is robust to imperfect reciprocity and resolves the threat of nearby eavesdroppers.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, pp. 1355–1387, Jan. 1975.

[2] P. Gopala, L. Lai and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory* , vol. 54, pp. 4687–4698, Oct. 2008.

[3] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

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

[5] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[6] H. Li, X. Wang, and J. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb. 2015.

[7] 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, Jul. 2009.

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

[9] S. R. Aghdam, T. M. Duman and M. Di Renzo, "On secrecy rate analysis of spatial modulation and space shift keying," *IEEE BlackSeaCom 2015*, Constanta, Romania, May 2015, pp. 63–67.

[10] S. R. Aghdam and T. M. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 180–183, Apr. 2016.

[11] Q.-L. Li, "Information-guided randomization for wireless physical layer secure transmission," in *Proc. IEEE Military Commun. Conf.*, Orlando, FL, USA, Nov. 2012, pp. 1–6.

[12] F. Wu, L. L. Yang, W. Wang and Z. Kong, "Secret precoding-aided spatial modulation," in *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544–1547, Sep. 2015.

[13] Y. Chen, L. Wang, Z. Zhao, M. Ma and B. Jiao, "Secure multiuser MIMO downlink transmission via precoding-aided spatial modulation," in *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1116–1119, Jun. 2016.

[14] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1351–1354, Aug. 2015.

[15] D. Qin and Z. Ding, "Exploiting multi-antenna non-reciprocal channels for shared secret key generation," in *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2693–2705, Dec. 2016.

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

[17] K. S. Ahn, R. Heath, and H. K. Baik, "Shannon capacity and symbol error rate of space-time block codes in MIMO Rayleigh channels with channel estimation error, *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 324–333, Jan. 2008.

[18] M. K. Simon and M. S. Alouini, "On the difference of two chi-square variates with application to outage probability computation," in *IEEE Trans. Commun.*, vol. 49, no. 11, pp. 1946–1954, Nov. 2001.

[19] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction," in *Proc. ACM Eur. Workshop Syst. Secur. (EUROSEC)*, New York, NY, USA, Apr. 2011, pp. 1–6.