

# “The Medium is The Message” : Secure Communication via Waveform Coding in MIMO Systems

Xin Zhou, Persefoni Kyritsi, Patrick Claus Friedrich Eggers, Frank Hanns Paul Fitzek  
Antenna, Propagation and Radio Networking Section, Department of Electronic Systems  
Aalborg University  
Aalborg, Denmark  
Email : {xz, persa, pe, ff}@kom.aau.dk

**Abstract**—In this paper, we look at multiple antenna systems and code information on the communication medium itself to improve the link security. In the case of single data stream transmission, the medium refers to the response across the receive sensor array. In multiple data stream transmission, the medium is the set of virtual orthogonal channels that result from the singular value decomposition of the channel transfer matrix. We code phase information on the orthogonal channels by rotating the received signal constellation. This does not impair the signal detection of differential-phase coded signals on the intended receiver. However the rotation at an eavesdropper location is different from the one on the intended receiver even at a distance of  $\frac{\lambda}{10}$ (6mm), and therefore security is enhanced.

## I. INTRODUCTION

In wireless communications, the information is conveyed from a central access point to terminals within its range. In the absence of additional measures to guarantee the link security, the content of the communication is susceptible to interception. As security concerns gain attention, the issue has been commonly addressed in higher layers of the communication stack, such as HyperText Transfer Protocol Secure (HTTPS) and Internet Protocol (IP) Security. With the introduction of IEEE 802.11 based wireless local area networks, the security was provided by even lower layers of the International Standard Organization’s Open System Interconnect (ISO/OSI) protocol stack. The first realization such as Wired Equivalent Privacy protocol (WEP) has been proven to be too weak with respect to security [1]. Therefore, more complex protocols are introduced such as Wireless Application Protocol (WAP) and Wi-Fi Protected Access 2 (WPA2) to offer more secure communication. The drawback is that these mechanisms are highly complex and result in increased device cost and battery consumption.

In this work we advocate to secure the wireless communication at the lowest ISO/OSI protocol layer, the physical one. Our approach follows the concept of *wireless fingerprinting*. It utilizes the communication medium to carry overlay information [2], on top of the baseline communication which should be undisturbed. This additional information can either be part of the transmitted data in order to increase the rate performance, or an encryption key so as to enhance the link security. In this

paper, we concentrate on the security properties of waveform coding and not capacity benefits.

We assume that multiple antennas are available at both the transmitter (Tx) side and at the receiver (Rx) side. It is already widely known that multiple input multiple output (MIMO) systems have significant benefits in terms of rate performance if spatial multiplexing is used [3]- [4], and fading mitigation if diversity is employed [5]- [8]. Our scheme uses the Tx antennas to control the waveform and the Rx antennas to detect the coded waveform, and add on to the high rate capability.

We look at single and multiple data stream transmission separately. Single data stream transmission is presented for reasons of illustration of principle. In this case, the “medium” refers to the receiver sensor response. In multiple data stream transmission, the baseline communication comprises multiple data streams, which are transmitted along the virtual orthogonal channels that result from the singular value decomposition (SVD) of the channel transfer matrix. Therefore the “medium” is this set of virtual orthogonal channels.

We assume that the overlay information is coded in the relative phase coding of the virtual orthogonal channels, and that the baseline communication also uses phase shift keying (PSK) modulation techniques. Our objective is to quantify how much phase information can be coded in the overlay mode so that a certain probability of error is achieved during the overlay information detection. Specifically, we want to find how many additional phase states can be tolerated in any constellation diagram for a predefined probability of symbol/block error. Then we assume that an eavesdropper close to the intended receiver also tries to find this phase rotation of the baseline communication. This will help us quantify the security potential of our scheme.

Several assumptions are made in this paper. We assume that the channel state information is perfectly probed and synchronized at the Tx side. The propagation channel is assumed to be Rayleigh flat-fading (no frequency variation). Perfect down-conversion, filtering and sampling have been performed. In addition, we assume that the same error rate performance is desired for both the baseline and the overlay communication.

## II. BASE AND OVERLAY COMMUNICATION IN MIMO SYSTEM

Let us first introduce the notation used in this paper. Bold and underlined symbols indicate matrices and vectors, respectively.  $(\cdot)^T$ ,  $(\cdot)^*$  and  $(\cdot)^H$  denote the transpose, conjugate and complex conjugate transpose (hermitian) of the argument  $(\cdot)$ , respectively.

We assume that baseline and overlay communication in a MIMO system are simultaneously achieved. Base communication refers to conventional signal processing and overlay communication indicates the waveform coding procedure.

Let us assume that we have a MIMO system with  $N_{TX}$  transmitter and  $N_{RX}$  receiver antennas. The input and output vectors are  $\underline{x} = [x_1 \ x_2 \ \dots \ x_{N_{RX}}]^T$  and  $\underline{y} = [y_1 \ y_2 \ \dots \ y_{N_{RX}}]^T$ , respectively. The transmitted signal vector  $\underline{s}$  is derived from the weighting of the information signal  $x$  as  $\underline{s} = \mathbf{W}\underline{x}$ . The received signal vector  $\underline{r}$  is given as :

$$\underline{r} = \mathbf{H}\underline{s} + \underline{n} = \mathbf{H}\mathbf{W}\underline{x} + \underline{n} \quad (1)$$

where  $\mathbf{H}$  is the  $N_{RX} \times N_{TX}$  dimensional channel transfer matrix. Each element  $H_{ij}$  of the channel transfer matrix  $\mathbf{H}$  corresponds to the gain from the  $j$ -th transmit antenna to the  $i$ -th receiver element, and is a complex scalar quantity.  $\underline{n}$  is the  $N_{RX}$ -dimensional noise vector. Its components are assumed to be additive, white, circularly symmetric complex Gaussian random variables with variance  $\sigma^2$ , independent across the receivers.

### A. Single Data Stream Transmission

In single data stream transmission, the transmitter sends the signal in a way which maximizes the received power at a target antenna. The receiver detects the response on all its sensors, and identifies the one where the received signal is maximized. This index carries the overlay information, which is in this case amplitude coded. Therefore, the response across the sensors becomes the “medium”.

In order to achieve power maximization on the target antenna, we use conventional beamforming. For example, if we focus on the  $k$ -th receiver antenna, then the transmitter weighting vector is  $\underline{w}_k = [H_{k1}^*, H_{k2}^*, \dots, H_{kN_{TX}}^*]$ . No cooperation between receiver antennas is required for the signal detection, keeping the receiver complexity low. Potentially the receiver could use diversity combining of the signals received on all its sensors, and that would result in higher complexity.

### B. Multiple Data Stream Transmission

We discuss multiple data stream transmission based on the concept of spatial multiplexing (see Fig. 1). The base communication refers to the transmission of several spatially multiplexed data streams transmitted along the virtual orthogonal channels that result from the application of the SVD technique at both the transmit and the receive sides. These virtual orthogonal channels constitute our transmission “medium”. The overlay communication is implemented along this medium through phase coding.

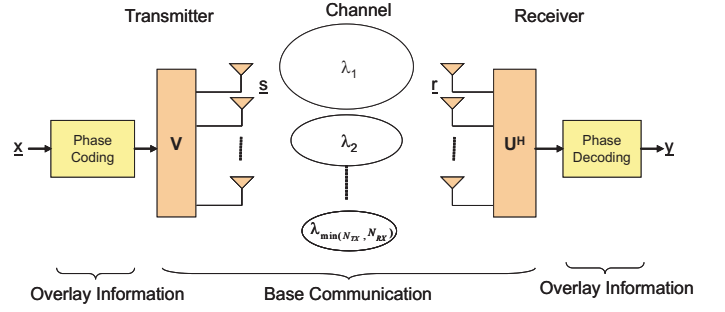


Fig. 1. Orthogonal transmission diagram in a  $N_{TX} \times N_{RX}$  MIMO System with phase coding via virtual orthogonal channels.

1) *Base Communication*: Let the singular value decomposition of the channel transfer matrix  $\mathbf{H}$  be

$$\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H. \quad (2)$$

The unitary matrices  $\mathbf{V}$  and  $\mathbf{U}$  contain the right (input) and left (output) singular vectors of  $\mathbf{H}$ , respectively.  $\mathbf{\Lambda}$  is a diagonal matrix with diagonal elements  $\lambda$ , which are the singular values of  $\mathbf{H}$ .

Let us first look at the received signals on the intended user.

$$\underline{r} = \mathbf{H}\underline{s} + \underline{\tilde{n}} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H\mathbf{V}\underline{x} + \underline{\tilde{n}} = \mathbf{U}\mathbf{\Lambda}\underline{x} + \underline{\tilde{n}} \quad (3)$$

$$\underline{y} = \mathbf{U}^H\underline{r} = \mathbf{U}^H\mathbf{U}\mathbf{\Lambda}\underline{x} + \mathbf{U}^H\underline{\tilde{n}} = \mathbf{\Lambda}\underline{x} + \underline{n} \quad (4)$$

The received signal of the  $k$ -th data stream is :

$$y_k = \lambda_k x_k + n_k, \quad (5)$$

We define the pre-detection average signal to noise ratio ( $SNR$ ) as :

$$SNR^{pre} = \frac{P_t}{\sigma^2} \langle |\mathbf{H}|^2 \rangle \quad (6)$$

where  $P_t$  denotes the total transmitted power.  $\langle \cdot \rangle$  is the expectation operator. The post detection  $SNR$  for the  $k$ -th data stream is calculated as :

$$SNR_k^{target} = \frac{P_S}{P_N} = \frac{|\lambda_k|^2 \cdot P_k}{\sigma^2} \quad (7)$$

where  $P_S$  and  $P_N$  denote the received signal and noise power, respectively.  $P_k$  is the transmit power allocated to the  $k$ -th orthogonal channel.

2) *Overlay communication*: The base communication refers to the symbol level transmission. We define the overlay communication on a block level (1 block =  $N_s$  symbols). This block information is encoded by rotating the phase of the constellation transmitted on the orthogonal subchannels by the same amount for all the symbols within the block. This corresponds to a multiplication by a term of the form  $e^{j\phi}$ .

We illustrate the concept with an example in Fig. 2. Let us assume that the baseline communication comprises the transmission of two data streams, which are transmitted using QPSK (Quadrature PSK) and BPSK (Binary PSK) respectively. To transmit the overlay information, we rotate the constellations relative to each other. Instead of transmitting along the aligned BPSK modulation as shown with a solid

line, we rotate the constellation diagram by a certain angle (dashed line). The ability of the system to discern the rotation angle defines the probability of error detection for the overlay communication.

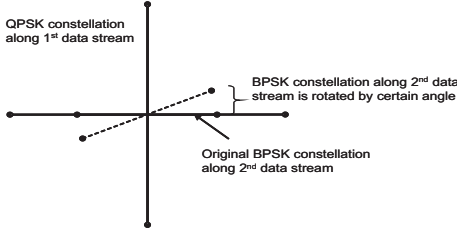


Fig. 2. Phase coding via 2nd orthogonal channel in a constellation diagram.

Using the previous notation, the signal on the  $k$ -th orthogonal channel is rotated by angle  $\phi_k$ :  $y_k = \lambda_k x_k e^{j\phi_k} + n_k$ , which does not change the resulting signal to noise ratio.

The phase rotation is estimated based on the estimated average received constellation points. Therefore the noise on the block level is the average of the noise on all  $N_s$  symbols in the block and its variance can be expressed as :

$$\sigma_b^2 = \frac{\sigma_s^2}{N_s} \quad (8)$$

where  $\sigma_b^2$  and  $\sigma_s^2$  denote the noise variance of one block and one symbol, respectively. The question now becomes how many bits can be coded on the overlay communication, or equivalently how many phase rotations can be detected with a pre-defined probability of error. To calculate that, we perform the following set of computations.

- 1) We send a block of  $N_s$  symbols along each eigenchannel assuming that the subchannels are not rotated relative to each other.
- 2) Each symbol in the block is impaired by additive noise, and is decoded. We group the received symbols into subsets, so that symbols within each set have been decoded to the same point from the original transmitted constellation. A way to implement this is by assuming that the baseline communication is differentially phase coded.
- 3) Within each subset, we average the complex received symbols (including the noise) to get an estimate of the true constellation point location.
- 4) The estimated constellation points differ from the true ones by rotation and dilation. We record only the rotation angle.
- 5) We repeat the calculation above for several blocks of symbols and observe the statistics of the rotation angle.
- 6) We find the outage angle  $\alpha_{min}$  by which the estimated constellation points are rotated with a target outage probability.

The number of allowable phase rotations of the original constellations that can be detected with that target outage

probability ( $N_{rot}$ ) is calculated as :

$$N_{rot} = \left\lceil \frac{\alpha_{max}}{2\alpha_{min}} \right\rceil \quad (9)$$

where  $\alpha_{max}$  is the angle difference between two adjacent constellation points for the constellations used for the base communication.  $N_{rot}$  indicates how many bits can be carried in the overlay communication per each rotation angle, namely  $\log_2 N_{rot}$ .

### C. Base and overlay communication at an eavesdropper location

Let us assume that the transmit weights are determined with a view to communicating to a target user. An eavesdropper at a nearby location tries to intercept the content of the baseline and the overlay communication by projecting on the output eigenvectors of the channel transfer matrix  $\hat{\mathbf{H}}$  to its location (see Fig. 3).

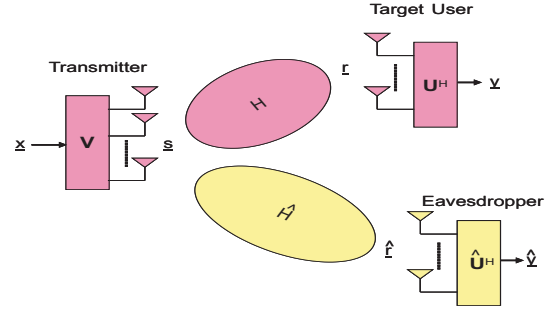


Fig. 3. Virtual orthogonal transmission diagram at the target user and eavesdropper locations.

The received signal at the eavesdropper location is

$$\hat{\mathbf{r}} = \hat{\mathbf{H}}\mathbf{s} + \hat{\mathbf{n}} = \hat{\mathbf{U}}\hat{\mathbf{\Lambda}}\hat{\mathbf{V}}^H\mathbf{V}\mathbf{x} + \hat{\mathbf{n}}, \quad (10)$$

$$\hat{\mathbf{y}} = \hat{\mathbf{U}}^H\hat{\mathbf{r}} = \hat{\mathbf{\Lambda}}\hat{\mathbf{V}}^H\mathbf{V}\mathbf{x} + \hat{\mathbf{U}}^H\hat{\mathbf{n}} \quad (11)$$

The received signal of the  $k$ -th data stream is :

$$\hat{y}_k = \hat{\lambda}_k \hat{\mathbf{v}}_k^H \mathbf{v}_k x_k + \sum_{j=1, j \neq k}^{\min(N_{TX}, N_{RX})} \hat{\lambda}_k \hat{\mathbf{v}}_k^H \mathbf{v}_j x_j + \hat{n}_k, \quad (12)$$

If the  $k$ -th orthogonal channel is rotated by angle  $\phi_k$  then this is interpreted at the eavesdropper location as :

$$\hat{y}_k = \hat{\lambda}_k \hat{\mathbf{v}}_k^H \mathbf{v}_k x_k e^{j\phi_k} + \sum_{j=1, j \neq k}^{\min(N_{TX}, N_{RX})} \hat{\lambda}_k \hat{\mathbf{v}}_k^H \mathbf{v}_j x_j + \hat{n}_k \quad (13)$$

### III. CHANNEL MODEL

The radio channel is simulated using a double bounce flat-fading Rayleigh model, with 100 scatterers on each scatter ring (20m radius) around the Tx and Rx, where the separation between the Tx and Rx is 30m. The center frequency is 5GHz (wavelength  $\lambda=6$ cm). The Tx and Rx use uniform linear antenna arrays, with  $\frac{\lambda}{2}$  element spacing. The Tx is static and the Rx moves along 100 tracks perpendicular to the antenna array, with a movement step of  $\frac{\lambda}{2}$ . The spacing between different tracks is  $0.4\lambda$ .

#### IV. PERFORMANCE EVALUATION

We set the target probability of symbol error ( $P_{s,e}$ ) and block error ( $P_{b,e}$ ) to  $10^{-3}$  and assume that our systems have a  $SNR^{pre}$  of 12dB. Thus the pre-detection  $SNR$  on the overlay communication equals to  $\lceil 10 + 10 \log_{10}(N_s) \rceil$  dB.

##### A. Single Data Stream

In single data stream transmission, the Tx focuses on each Rx antenna at each time by coding the amplitude of the sensor response. We investigate the probability of error on the Rx antennas by varying the system size :  $4 \times 4$ ,  $8 \times 4$  and  $16 \times 4$ , assuming 100 symbols per block. As shown in Fig. 4, the size of antenna system increases, the error rate decreases. However, even  $16 \times 4$  system can not achieve the  $10^{-3}$  error rate.

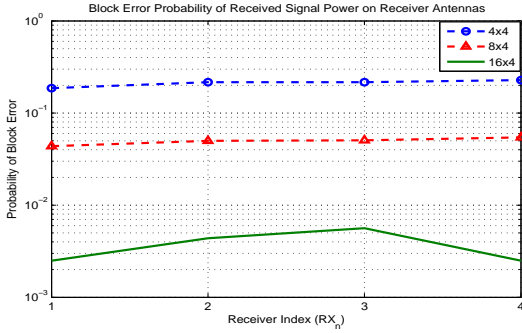


Fig. 4. Block error probability of received signal power on receiver antennas in a  $N_{TX} \times 4$  MIMO system.

##### B. Multiple Data Streams

We look at a  $4 \times 4$  MIMO system, to calculate how much the constellation diagrams can be rotated so as to achieve a certain probability of error of  $10^{-3}$  for the overlay communication, under the assumption that the system operates at a pre-detection  $SNR$  of 12dB.

The first question is how the modulation size is determined for the baseline communication because that will determine the angle  $\alpha_{max}$ . The transmitter does not perform power waterfilling on the eigenchannels. Because the channel gains of the eigenchannels are not equal ( $\lambda_1 > \lambda_2 > \lambda_3 > \lambda_4$ ), without waterfilling the third and fourth eigenchannels can not achieve  $P_{s,e} = 10^{-3}$  even for the lowest modulation order of BPSK. Thus only the two strongest eigenchannels (with gains  $\lambda_1$  and  $\lambda_2$ ) are used and the transmit power is equally divided between them, namely  $P_1 = P_2 = \frac{P_t}{2}$ .

Our analysis shows that the average  $SNR$  for the first eigenchannel is 19dB and therefore a 8PSK constellation can be transmitted at the target probability of error of  $10^{-3}$  [9]. In that case adjacent symbols in the constellation are separated by  $22.5^\circ (= \lceil \frac{360^\circ}{8 \times 2} \rceil)$ . The average  $SNR$  for the second eigenchannel is 14dB and therefore a QPSK constellation can be transmitted while satisfying the target probability of error of  $10^{-3}$ . In that case adjacent symbols in the constellation are separated by  $45^\circ (= \lceil \frac{360^\circ}{4 \times 2} \rceil)$ .

We implement the procedure defined in section II.B. Fig. 5 shows the Complementary Cumulative Distribution Function (CCDF) of  $\alpha_{min}$ . At  $P_{b,e}=10^{-3}$ , the outage phase between the two constellations should be at least  $7.8^\circ$  and  $2.3^\circ$  isolation, for a block size of 100 symbols or 1000 symbols respectively. Thus the number of phase rotations ( $N_{rot}$ ) that can be coded is  $2 (= \lceil 1 + \frac{22.5^\circ}{2 \times 7.8^\circ} \rceil)$  and  $5 (= \lceil 1 + \frac{22.5^\circ}{2 \times 2.3^\circ} \rceil)$ , respectively.

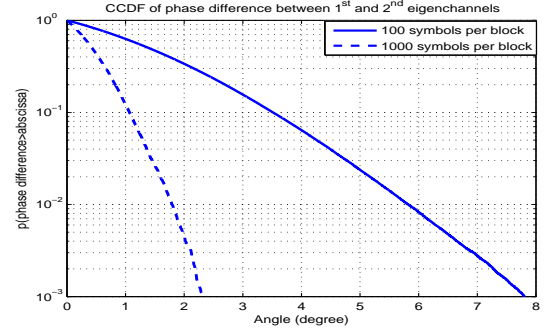


Fig. 5. CCDF of phase difference in overlay communication.

##### C. Security performance

In this section, we evaluate the security performance of our proposed scheme by looking at the signal at an eavesdropper location. We apply the 8PSK and QPSK modulation schemes for the  $1^{st}$  and  $2^{nd}$  eigenchannels, respectively.

###### 1) Effect of rotation angle

Let us assume that the distance between the target user and the eavesdropper is  $\frac{\lambda}{5}$  (12mm), and that the second virtual orthogonal channel (along  $\lambda_2$ ) is rotated by either  $0^\circ$  or  $22.5^\circ$ . Fig. 6 shows the received signal constellations at the target user (upper row) and at the eavesdropper (lower row). At the target, the subsets of each eigenchannel are clearly separated based on the corresponding modulation schemes. At the eavesdropper, the difference between the subsets is ambiguous, which leads to high error probability.

###### 2) Effect of target–eavesdropper separation

Fig. 7 shows constellation diagrams of the received signals as observed at eavesdropper locations  $\frac{\lambda}{50}$  (1.2mm),  $\frac{\lambda}{10}$  (6mm),  $\lambda$  (6cm) and  $5\lambda$  (30cm) away from the intended user, when the rotation angle on the  $2^{nd}$  virtual channel of the target user is  $22.5^\circ$ . The diagram of the target user at this time is shown in Fig. 6 (right upper figure with  $\phi_1=0^\circ$ ,  $\phi_2=22.5^\circ$ ).

When the eavesdropper is  $\frac{\lambda}{50}$  away from the target user, the symbols are grouped into different subsets and the constellation diagram looks similar to that of the target user. When the distance between the target user and the eavesdropper is as low as  $\frac{\lambda}{10}$ , the separation of the subsets for the  $1^{st}$  eigenchannel is no longer clear. As the distance to the eavesdropper increases, the ambiguity of different subsets in both eigenchannels increases and higher error probability occurs.

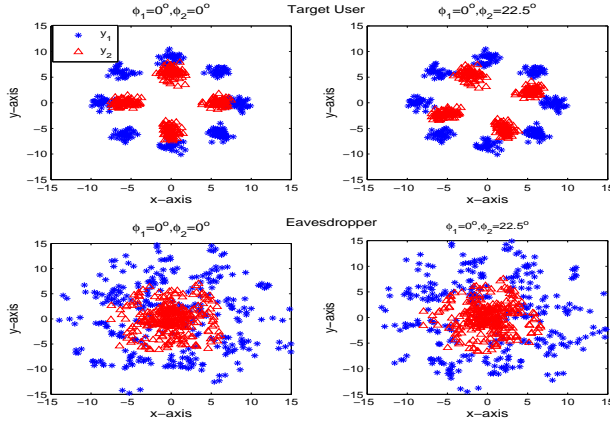


Fig. 6. Constellation diagram at the target user and at an eavesdropper if the  $2^{nd}$  virtual channel is rotated by  $0^\circ$  and  $22.5^\circ$ . The distance between the target user and the eavesdropper is  $\frac{\lambda}{5}$  (12mm).

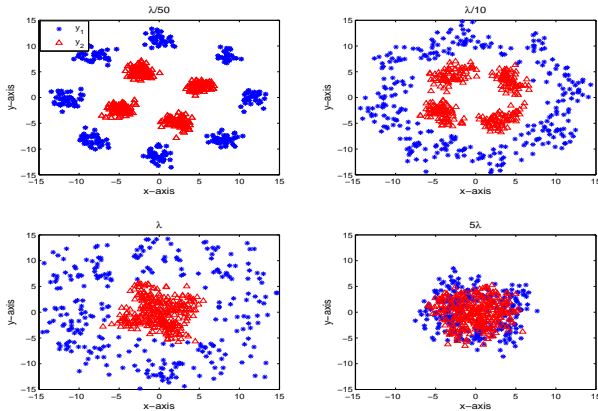


Fig. 7. Constellation diagram at eavesdropper for different distances from the target ( $\frac{\lambda}{50}$  (1.2mm),  $\frac{\lambda}{10}$  (6mm),  $\lambda$  (6cm) and  $5\lambda$  (30cm)). The stream along the  $2^{nd}$  eigenchannel has been rotated by  $22.5^\circ$ .

### 3) Probability of error on the overlay communication

We calculate the probability of symbol error for the overlay communication with respect to the distance between the target user and eavesdropper. We use 8PSK and QPSK modulations for the baseline communication (8PSK-QPSK), and use the BPSK modulation scheme to encode/ decode the overlay information. As seen from Fig. 8, when the target user is  $\frac{\lambda}{100}$  far away from the target user, the probability of error for the overlay communication is approximately 4%. As the distance increases greater than  $\frac{\lambda}{10}$  (6mm), the probability of error tends to 50%. This indicates that the eavesdropper can not detect the correct user information, even with a distance of  $\frac{\lambda}{10}$  and high security of the overlay information is achieved. In order to achieve low error probability, we back off the modulation size of the base communication to QPSK and BPSK for the  $1^{st}$  and  $2^{nd}$  eigenchannel, respectively. As seen from Fig. 8, the error probability

is lower than 1% within a range of  $\frac{\lambda}{100}$  from the target user, which provides robustness of the baseline communication. As the number of symbols per block increases, the probability of error for the overlay communication decreases, since the noise variation becomes smaller.

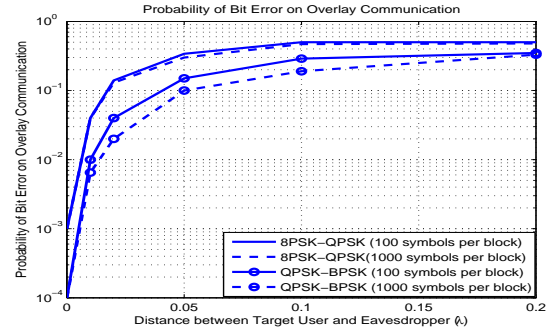


Fig. 8. Probability of bit error on overlay communication with respect to the distance between the target user and eavesdropper. The modulation schemes on the baseline communication are 8PSK-QPSK and QPSK-BPSK.

## V. CONCLUSION

In this paper, we investigated the possibility of employing the communication medium as bearer of useful information. In single data stream transmission, the overlay information is the amplitude coding of the waveform, by using conventional beamforming to maximize the received signal power on the target receiver antenna. The results show that the larger the antenna system size, the fewer errors occur. In multiple data stream transmission, the overlay information is the phase coding on top of the SVD method. Even at a separation of  $\frac{\lambda}{10}$ , the eavesdropper has prohibitively high bit error rate, which achieves secure communication.

## REFERENCES

- [1] S.R. Fluhrer, I. Mantin and A. Shamir, "Weakness in the key scheduling algorithm of RC4," Lecture notes in Computer Science, vol. 2259. Revised papers from the 8th Annual International Workshop on Select. Areas in Cryptography, pp. 1-24, 2001.
- [2] F.H.P. Fitzek, "The medium is the message," in *IEEE International Conference on Communication (ICC)*, 2006.
- [3] I.E. Telatar, "Capacity of Multi-antenna Gaussian Channels," AT&T Bell Laboratories, Murray Hill, NJ, Technical note, 1996.
- [4] J.B. Andersen, "Array gain and capacity for known random channels with multiple element arrays at both ends," in *IEEE J. Select Areas Commun.*, vol. 18, pp. 2172-2178, Nov. 2000.
- [5] Lizhong Zheng and D.N.C. Tse, "Diversity and multiplexing : a fundamental tradeoff in multiple-antenna channels," in *IEEE Trans. on Inform. Theory*, vol. 49, no. 5, 1073-1096, May 2003.
- [6] R.W. Heath, Jr. and A.J. Paulraj, "Switching between diversity and multiplexing in MIMO systems," in *IEEE Trans. on Commun.*, vol. 53, no. 6, June 2005.
- [7] E. Sengul, E. Akay and E. Ayanoglu, "Diversity analysis of single and multiple beamforming," in *IEEE Trans. on Commun.*, vol. 54, Issue 6, pp.990-993, June 2006.
- [8] D.J. Love, R.W. Heath, Jr. and T. Strohmer, "Grassmannian Beamforming for multiple-input multiple output wireless systems," in *IEEE Trans. on Inform. Theory*, vol. 49, no. 10, 2735-2747, Oct. 2003.
- [9] J.G. Proakis, "Digital Communications," McGraw-Hill International Editions, pp. 170, 1987.