2011 International Symposium on Nonlinear Theory and its Applications
NOLTA2011, Kobe, Japan, September 4-7, 2011

A comparative study of bit error rate performance in chaos MIMO transmission system

Eiji Okamoto
Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya, 466-8555 Japan

Abstract—**A chaos multiple-input multiple-output (C-MIMO) transmission scheme which is a chaotic channel coding scheme between multiple transmit antennas of MIMO multiplexing, achieves a high-capacity and secure wireless communication. We consider the chaos configuration of C-MIMO and investigate the coding characteristics including bit error rate performances. Since a square Euclidean distance property changes according to the configuration of chaos vector and chaos composition, we conduct a heuristic search and clarify a good configuration. In addition, we describe a concept of personal modulation using this chaos transmission.**

Keywords-chos coding; multiple-input multiple-output; maximum likelihood decoding; Bernoulli shift map; Tent map.

I. INTRODUCTION

In wireless communication systems, as an increasing ability of signal processing, a nonlinear processing is more and more applied to achieve an improved performance. A maximum likelihood decoding (MLD) is a representative example of it. An optimum solution in terms of decoding error probability is obtained by searching all candidates of transmit sequences in MLD. However, the number of candidates increases exponentially for the degree of freedom on transmit sequences and the calculation complexity tends to diverge. Hence, the complexity is kept within an allowable range by restricting a magnitude of degree of freedom in general.

A multiple-input multiple-output (MIMO) transmission system [1] where multiple antennas are used in a terminal is one of the major systems in which MLD is applied. By MIMO property of antenna multiplexing and/or antenna diversity without an increase of radio bandwidth, a higher-capacity and higher-quality transmission is achieved, and the MIMO is widely used as a standard technique in such as cellular phone or wireless LAN systems recently.

Here, a wireless security also becomes important recently due to the transmission of personal information or the application of multihop transmission systems. It is important not to disclose information to the third person. However, in the current systems, ensuring the security is achieved on upper layer such as XOR-scrambling generated by a common key and the physical-layer security is not put to practical use. We utilized the property of chaos communication [2-8] and proposed a chaos MIMO (C-MIMO) transmission scheme achieving the physical-layer security, channel coding gain, and MIMO increased capacity by MLD [9]. This scheme conducts a chaotic channel coding between transmit antennas of MIMO multiplexing transmission and those three properties are simultaneously obtained by MLD. In the study of [9], however, only one configuration of chaos has been considered and the relationship between transmission performances and the chaos configuration is not clarified. Therefore, in this paper, we analyze the relationship between chaos configuration of C-MIMO and the square Euclidean distance dominating bit error rate (BER) performances in MLD by computer simulations. Then, we briefly describe an applicable concept of 'personal modulation' using chaos for a wireless security.

II. CHAOS MIMO SYSTEM

A. System model

The proposed scheme exploits MIMO multiplexing and chaos coding that enables the MIMO diversity effect and the physical-layer security. Fig. 1 shows the baseband system model of C-MIMO where N_t and N_r are the numbers of transmit and receive antennas, respectively. As shown in the figure, the proposed system is basically the same as conventional MIMO multiplexing system except the multiplication of chaos symbols at chaos encoder. In this scheme, a block transmission which consists of multiple MIMO vectors is used and the decoding at the receiver is done by this block unit. The number of MIMO vectors on one block is B and the bits to be transmitted on the block is

$$\boldsymbol{b} = [b(0) \cdots b(K-1)], \ b(l) \in \{0,1\} \tag{1}$$

where K is a number of bits per block. If the point of modulation constellation is $A = 2^q$, K becomes $K = qB$ and we consider BPSK ($q = 1$) case here. The data bits are serial-to-parallel transformed and loaded to each antenna. Then, the modulated symbols $s_j(k)$ are generated where k ($0 \le k \le B-1$) is the time and j ($1 \le j \le N_t$) is the antenna index. When the transmit symbol vector at time k is written by

$$\boldsymbol{s}(k) = \left[s_1(k) \cdots s_{N_t}(k) \right]^T \tag{2}$$

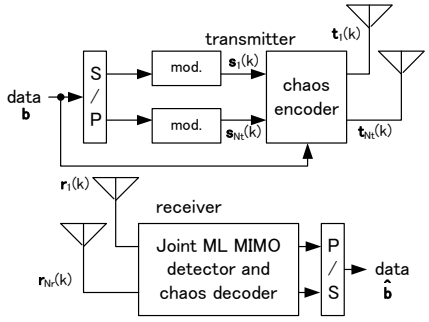


Fig. 1. Chaos MIMO system model.

then, the transmit block matrix becomes

$$\boldsymbol{S} = \left[\boldsymbol{s}(0) \cdots \boldsymbol{s}(B-1)\right] \tag{3}$$

where T is a matrix transpose. The transmit block is then encrypted by a chaos matrix as follows.

$$\begin{aligned} \boldsymbol{T} &= \left[\boldsymbol{t}(0) \cdots \boldsymbol{t}(B-1)\right] \\ &= \boldsymbol{C} \circ \boldsymbol{S} \end{aligned} \tag{4}$$

$$\boldsymbol{C} = \begin{bmatrix} c(1) & \cdots & c\left(\{B-1\}N_t+1\right) \\ \vdots & \ddots & \vdots \\ c(N_t) & \cdots & c\left(BN_t\right) \end{bmatrix} \tag{5}$$

Here, $\circ$ means scalar product (Hadamard product) of each element and $c(k)$ is the encoded chaos symbol. Finally, $\boldsymbol{T}$ is transmitted. The generation of chaos matrix $\boldsymbol{C}$ is described later. This multiplication is the same as a space-time block coding (STBC) without a loss of transmission efficiency. That is, a MIMO multistream transmission and coding are achieved. It is assumed that the MIMO channel is an i.i.d. quasi-static fading between every antennas and on every MIMO symbols. This symbol i.i.d. assumption will be satisfied by some additional interleavers in practical systems. The channel matrix is given by

$$\boldsymbol{H}(k) = \begin{bmatrix} h_{11}(k) & \cdots & h_{1Nt}(k) \\ \vdots & \ddots & \vdots \\ h_{Nr1}(k) & \cdots & h_{NrNt}(k) \end{bmatrix} \tag{6}$$

and the receive block ($N_r \times B$)-matrix is composed by

$$\boldsymbol{R} = \left[\boldsymbol{r}(0) \cdots \boldsymbol{r}(B-1)\right],\ \boldsymbol{r}(k) = \left[r_1(k) \cdots r_{N_r}(k)\right]^T \tag{7}$$

where $r_i(k)$ is the receive symbol of i-th antenna. The noise block is similarly given by

$$\boldsymbol{N}(k) = \left[\boldsymbol{n}(0) \cdots \boldsymbol{n}(B-1)\right],\ \boldsymbol{n}(k) = \left[n_1(k) \cdots n_{N_r}(k)\right]^T \tag{8}$$

where each $n_i(k)$ is i.i.d. additive white Gaussian noise (AWGN). Then, the receive vector can be written by

$$\boldsymbol{r}(k) = \boldsymbol{H}(k)\boldsymbol{t}(k) + \boldsymbol{n}(k) \tag{9}$$

In the receiver, the joint maximum likelihood (ML) MIMO detection and chaos decoding is conducted by

$$\hat{\boldsymbol{b}} = \arg\min_{\boldsymbol{b}} \left\| \boldsymbol{R} - \boldsymbol{H}\boldsymbol{T} \right\|_F^2 \tag{10}$$

$$\boldsymbol{H} = \left[\boldsymbol{H}(0) \cdots \boldsymbol{H}(B-1)\right],\ \boldsymbol{T} = \begin{bmatrix} \boldsymbol{t}(0) & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{t}(1) & & \\ \vdots & & \ddots & \vdots \\ \boldsymbol{0} & \cdots & & \boldsymbol{t}(B-1) \end{bmatrix}$$

where $\|\cdot\|_F$ is the Frobenius norm and from (1), the number of decoding search becomes 2^K.

B. Chaos encoder

In this paper, we use Bernoulli shift map and Tent map [3] to generate chaos signals for easy signal processing. The following two types of chaos encoding vector in chaos matrix of (5) are considered.

$$c(k) = \exp\left\{ j2\pi \tan^{-1}\left(\mathrm{Im}[s_k]/\mathrm{Re}[s_k]\right)\right\} \tag{11a}$$

$$c(k) = s_k \tag{11b}$$

The former is a unit vector and the latter is a Gaussian vector. Here, s_k is the pseudo-Gaussian noise vector obtained by

$$s_k = \frac{1}{M}\sum_{i=0}^{M-1}\left\{(\mathrm{Re}[c_{ki}] + \mathrm{Im}[c_{ki}])\exp(j8\pi[\mathrm{Re}[c_{ki}] - \mathrm{Im}[c_{ki}])\right\} \tag{12}$$

where k is $1 \le k \le BN_t$ and c_{ki} is an M-element chaos symbol used to generate Gaussian distribution. M is the number of independent chaos signals used for making white noise by central limit theorem, and is set to relatively large value. In (11a), since $c(k)$ is a unit vector, the encryption of $\boldsymbol{S}$ is conducted by the random phase shift which doesn't change the average transmit power. In the case of (11b), the encoded transmit symbol $t_j(k)$ becomes a random Gaussian vector. Each chaos symbol c_{ki} is given by M-element chaos vector as

$$\boldsymbol{c}_M(k) = [c_{k0} \cdots c_{k(M-1)}]\ ,\ \ c_{ki} \in \mathbb{C}\ ,\ \ 0 < \mathrm{Re}[c_{ki}], \mathrm{Im}[c_{ki}] < 1 \tag{13}$$

and the source and destination terminals have the same initial vector

$$\boldsymbol{c}_M(0) = [c_{00} \cdots c_{0(M-1)}] \tag{14}$$

Thus, the proposed scheme is categorized as the common key encryption and $\boldsymbol{c}_M(0)$ in (14) is the key signal, which can also be quantized. Then, the chaos vector $\boldsymbol{c}_M(k)$ is iteratively modulated by the chaos convolution with transmit data as

$$\boldsymbol{c}_M(k) = f\left(\boldsymbol{c}_M(k-1), \boldsymbol{b}_k\right) \tag{15}$$

where f is the iteration function and $\boldsymbol{b}_k$ is a partial cyclic shift version of data bits $\boldsymbol{b}$ given by

$$\begin{aligned} \boldsymbol{b}_k &= \left[b_k(1), \cdots, b_k(q)\right] \\ &= \left[b\left(\{k+K-q\} \bmod K\right), \cdots, b\left(\{k+K-1\} \bmod K\right)\right] \end{aligned}$$

The chaos transition of (15) is conducted independently in real and imaginary parts. The real part is given as follows.

$$x_0 = \begin{cases} \mathrm{Re}[c_{(k-1)i}] & \left(b_k(1) = 0\right) \\ \mathrm{Re}[c_{(k-1)i}] - 1/2 & \left(b_k(1) = 1,\ \mathrm{Re}[c_{(k-1)i}] > 1/2\right) \\ 1 - \mathrm{Re}[c_{(k-1)i}] & \left(b_k(1) = 1, \mathrm{Re}[c_{(k-1)i}] \le 1/2\right) \end{cases} \tag{16}$$

$$x_{l+1} = 2x_l \bmod 1 \tag{17a}$$

$$x_{l+1} = 1 - 2\left|x_l - 1/2\right| \tag{17b}$$

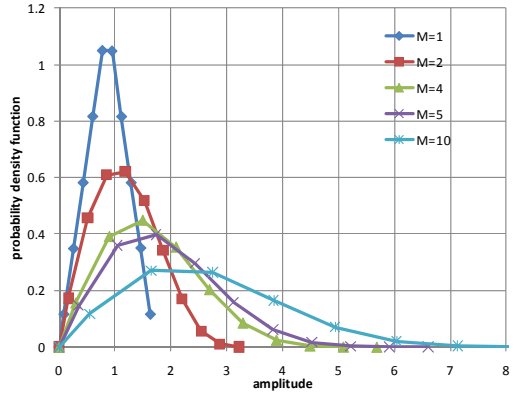
$$\mathrm{Re}[c_{ki}] = x_{Ite} \tag{18}$$

The operation of (16) is the chaos modulation. As shown in (18), the coding symbol c_{ki} is generated after Ite-th chaos iteration. The imaginary part is the same as (16)-(18) and only (17) is used for the imaginary part in BPSK. Eq. (17a) is the Bernoulli chaos shift transition and (17b) is the tent map function. Either of (17) functions is used in chaos encoder. This configuration of chaos was determined by numerical search and could be freely changed. However, since the BER performance is affected by this configuration, the squared Euclidean distance properties are evaluated in the next section.

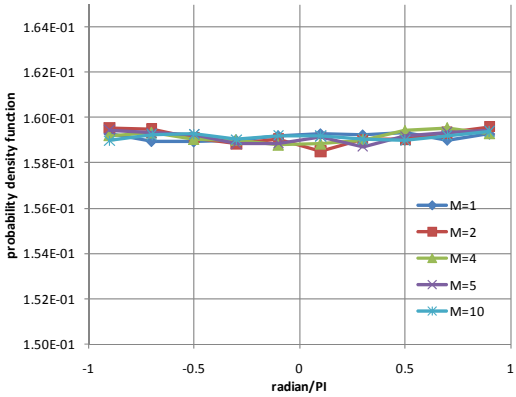
Here, a linear nulling scheme of inverse matrix multiplication exists for MIMO detection other than MLD as a low complexity scheme. However, since the chaos block coding is applied as shown in (4) and (5) in the proposed scheme, the symbol-by-symbol detection and decoding cannot be utilized and the sequential decoding of (10) is needed. To enable the symbol-by-symbol MIMO detection and decoding, the chaos coding should be symbol-by-symbol, that is, code constraint must be 1. In this case, however, the coding gain is not sufficiently obtained and the error rate performance is degraded. Thus, the MLD is adopted here.

III. NUMERICAL RESULTS

We confirm the performance changes by the configuration of chaos encoder through computer simulations. The proposed chaos encoding is a rate-one encoding and obtained the coding gain by enhancing the signal space from $\mathbb{C}$ to $\mathbb{C}^B$. Thus, from the point of view of random coding, the coding vector is desirable to have a Gaussian distribution. Hence, we calculate the distribution of pseudo-random vector s_k in (12) versus the number of chaos signals M. Fig. 2 shows the probability density functions (pdf) of amplitude (a) and phase (b). According to the increase of M, the pdfs converge on Rayleigh



(a)



(b)

Fig. 2. Probability density function of s_k: (a) amplitude distribution, (b) phase distribution.

distribution in (a) and uniform distribution in (b), respectively, due to the central limit theorem. It is found that M=5 is sufficient to obtain the complex Gaussian distribution on s_k of baseband vector. M=10 is used in the following consideration.

Next, the transmission performances are evaluated. It is assumed that the channel is perfectly known to the receiver. The square Euclidean distances of the right term of (10) are calculated with the parameters of chaos vector on (11), chaos equation on (17), the number of antennas, and the block length B. Here, the channel matrix is assumed as a unit matrix which is equivalent to virtual parallel lines of sight transmission, and the number of trials is 10^5. The normalized distance characteristics are listed in Tab. 1. In this table, the average square distance means the average square distance per one symbol of all decoding sequences in MLD and the average minimum square distance means the average square distance per one sequence of the neighbor decoding sequence having minimum distance. The iteration number *Ite* is fixed to 18. In the conventional BPSK-MIMO-MLD transmission, both distances become 4.0 and this is the reference whether the coding gain is obtained in the proposed scheme or not. From Tab. 1, it is found that the proposed scheme has almost a half average distance per one symbol of 2.0 for the conventional scheme regardless of configurations. This means that the cross-correlation of different signals becomes almost zero and the security of signals are ensured. Concurrently, it costs the distance shortening to a half of BPSK, equivalent to 3 dB degradation on BER performance. In the proposed scheme, this degradation is redeemed by the block coding and decoding as $B \geq 2$ where the minimum distance is proportional to B. Different from the average distance, the minimum square Euclidean distance is sensitive to the chaos configuration and it is found that the combination of unit vector (11a) and shift map (17a) has a coding gain (i. e., MIMO transmit diversity gain). On the other hand, the configuration of Gaussian vector (11b) has a similar average distance but also much smaller minimum distance than 2.0, resulting in BER degradation in MLD. To confirm it, the BER performances with N_t=N_r=2 and B=2 in a symbol i.i.d. Rayleigh fading channel are calculated.

Table 1. Square Euclidean distances of chaos-MIMO.

chaos symbol	chaos	ite. no.	Nt, Nr	B	avg. sq. distance	avg. min. sq. distance
unit vector (11a)	shift map	18	2	2	2.13	4.11
			2	3	2.03	4.14
			4	2	2.01	4.09
	tent map	18	2	2	2.13	4.00
			2	3	2.03	3.99
			4	2	1.95	2.66
Gaussi-an vector (11b)	shift map	18	2	2	2.13	2.00
			2	3	2.04	1.63
			4	2	2.00	1.37
	tent map	18	2	2	2.14	1.05
			2	3	2.03	0.90

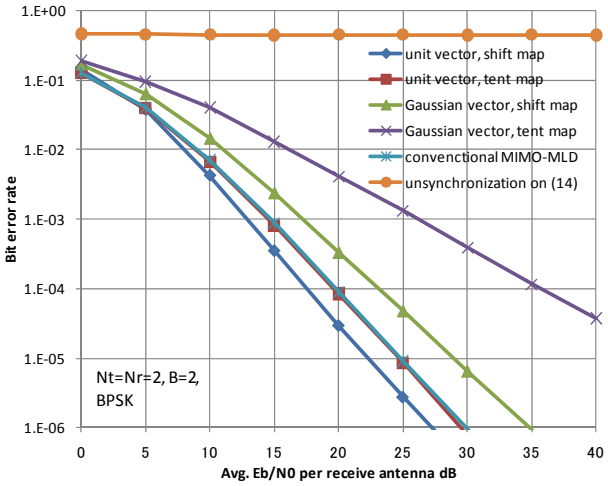


Fig. 3. BER performance of C-MIMO.

As shown in Fig. 3, the BER performances coincide the average minimum square Euclidean distance in Tab. 1. In addition to the security ability, C-MIMO with unit vector and shift map has 2.7 dB gain at BER of 10^{-5} for MIMO-MLD. However, the performances are identical or degraded in other settings.

Then, we focus on the unit vector with shift map, and calculate the distance characteristics versus the chaos iteration number *Ite*. From the result of Tab. 2, except for 50 iteration the distances don't drastically change. Therefore, by allocating different *Ite* for different users, this iteration number can also be a key information other than the initial chaos value of (14), and the security can be raised.

Here, to find another better configuration, we change the chaos modulation from (16) to

$$x_0 = \begin{cases} \mathrm{Re}[c_{(k-1)i}] & (b_k(1)=0) \\ 1-\mathrm{Re}[c_{(k-1)i}] & (b_k(1)=1) \end{cases} \qquad (19)$$

and calculate the distance characteristics. As a result, the average distance of 2.13 and the average minimum distance of 4.23 were obtained under the unit vector and shift map condition.

Consequently, from the simulation results we found that the distance characteristics change according to the chaos configuration and the combination of unit vector and shift map has a better performance. Also, there are numbers of settings having the average minimum distance over 4.0. Therefore, by utilizing this property, the chaos configuration can be treated as a key information only target transmitter and receiver share and the security will be increased. This property can be extended to a concept of 'personal modulation' where the modulation becomes a kind of personal ID and the physical-layer security is ensured.

IV. CONCLUSION

In this paper we considered the configuration of chaos encoder in C-MIMO and clarified their performances by computer simulations. Two types of chaos and unit or

Table 2. Square Euclidean distances for chaos iteration number.

chaos symbol	chaos	ite. no.	Nt, Nr	B	avg. sq. distance	avg. min. sq. distance
unit vector (11a)	shift map (17a)	10	2	2	2.13	4.10
		20			2.13	4.11
		30			2.13	4.10
		40			2.13	4.10
		50			2.12	3.78
		100			2.13	4.12
		200			2.13	4.11

Gaussian vector on chaos encoder were considered, and the square Euclidean distance characteristics were calculated. From the simulation results, it was found that the combination of unit vector and shift map had a better distance performance than MIMO-MLD and also it was confirmed by the BER comparison. Since there are several configurations having better distance characteristics, the chaos configuration can be treated as a key information which raises the physical-layer security and we introduced the concept of personal modulation.

For future study, the information theoretical security will be derived for C-MIMO when the chaos modulation is treated as the key.

REFERENCES

[1] G. J. Foschini, "Layered space–time architecture for wireless communication in a fading environment when using multiple antennas," Bell Labs Syst. Tech. J., vol. 1, pp. 41–59, 1996.

[2] T. L. Carroll, L. M. Pecora, "Synchronizing chaotic circuits," IEEE Trans. Cir. Sys., vol. 38, no. 4, pp. 453-456, Apr. 1991.

[3] B. Chen and G. W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," IEEE Trans. Comm., Vol. 46, Issue 7, pp. 881-890, Jul. 1998.

[4] H. Dedieu, M. P. Kennedy and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," IEEE Trans. Cir. Sys., vol. 40, no. 10, pp. 634–641, Oct. 1993.

[5] G. Kolumban and M.P. Kennedy, "Recent results for chaotic modulation schemes," Proc. IEEE Intl. symp. on Cir. Sys., vol. 3, pp 141–144, May 2001.

[6] S. Kozic, T. Schimming, and M. Hasler, "Controlled One- and Multidimensional Modulations Using Chaotic Maps," IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 53, no. 9, pp. 2048- 2059, 2006.

[7] R. Kharel, S. Rajbhandari, Z. Ghassemlooy, and K. Busawon, "Digitization of chaotic signal for reliable communication in non-ideal channels", Proc. Int'l Conf. on Transparent Optical Networks, Mediterranean Winter 2008 (ICTON- MW'08), pp. Sa1.2 (1-6), Dec., 2008.

[8] F. J. Escribano, L. López, and M. A. F. Sanjuán, "Iteratively decoding chaos encoded binary signals," in Proc. Eighth IEEE International Symposium on Signal Processing and Its Applications (ISSPA) 2005, vol. 1, Sydney, Australia, pp. 275-278, Aug. 2005.

[9] E. Okamoto, "A chaos MIMO transmission scheme for secure communications on physical layer," Proc. IEEE Vehicular Tech. Conf. 2011-Spring, 5 pages, May 2011.