PAPER

A Chaos MIMO Transmission Scheme for Channel Coding and Physical-Layer Security

Eiji OKAMOTO[†a)], ***Member***

SUMMARY In recent wireless communication systems, security is ensured mainly in the upper-layer techniques such as a password or a cryptography processing. However, security needs not be restricted to the upper-layer and the addition of physical-layer security also would yield a much more robust system. Therefore, in this paper, we exploit chaos communication and propose a chaos multiple-input multiple-output (MIMO) transmission scheme which achieves physical-layer security and additional channel-coding gain. A chaotic modulation symbol is multiplied to the data to be transmitted at each MIMO antenna to exploit the MIMO antenna diversity, and at the receiver, the joint MIMO detection and chaos decoding is done by maximum likelihood decoding (MLD). The conventional chaos modulation suffers from bit error rate (BER) performance degradation, while the coding gain is obtained in the proposed scheme by the chaos modulation in MIMO. We evaluate the performances of the proposed scheme by an analysis and computer simulations.

key words: *chaos coded modulation, MIMO, maximum likelihood decoding, convolutional code*

1. Introduction

The demands for higher-rate and higher-quality wireless communications have been growing. The higher-capacity wireless system enables more convenient services such as wireless money settlement services, real-time translation using mobile phone, telemedical consultation, and multimedia communications. An important factor in those services is security. To achieve the above services which demand information privacy the transmission data should not be decoded by any users except the intended users, and thus, secure communication is needed.

In the current systems, the security is ensured by such as the public key encryption [1] or IPsec [2] at the upper-layer and physical-layer security is not well utilized. However, ensuring security is never exclusive at each transmission layer and adopting multiple secure protocols enhances the security. As the physical layer security, a spread spectrum technique [3] has been established but it is used as code division multiple access (CDMA) scheme and is not used in security purpose.

Meanwhile, a chaos communication [2] is a well-known scheme ensuring the physical layer security. By adding the chaos signal to data signal or by modulating chaos signal by the data, the transmission signal becomes noise-like and the secure data transmission is achieved [3]. Although it is known that the security of chaos is not perfect, it can be increased by using multiple independent chaos signals [4]. Combining the chaos scheme with upper layer secure protocols consolidates the security and hence the chaos communication is an effective scheme to ensure the physical layer security. In conventional studies, the chaos schemes focusing on increasing the security have been proposed in [5] and [6]. These schemes achieve physical layer security but the bit error rate performance is degraded due to an extra power requirement of chaos signal. In [7] and [8], a chaotic convolutional coding was proposed to improve the error rate performance and also a chaos turbo code with parallel-concatenating two chaos convolutional codes was proposed in [9] and [10]. However, in this turbo code a number of chaos state is limited to apply maximum a posteriori (MAP) decoding [11], [12], resulting in a lower security. We also proposed a chaos coded modulation scheme in [13] enabling the physical layer security and channel coding gain without limiting a number of chaos states. The coding gain can be enhanced only by increasing decoding complexity. However, to obtain a large coding gain, the required decoding complexity becomes more than 2^{10}, which is relatively large. To address this problem, a complexity reduction scheme in [13] was proposed but the burst error occurred in decoding and the performance was degraded.

Here, applying chaos is available in any parts of signal processing on physical layer. A multiple-input multiple-output (MIMO) transmission scheme [14] in which multiple antennas are used in both transmitter and receiver is used in lots of recent wireless systems such as cellular or WLAN. There, MIMO is adopted as a mandatory standard technique. In MIMO multiplexing transmission, the channel capacity can be linearly increased in proportional to a number of antennas and a large capacity transmission is achieved. The receive signal on each MIMO antenna becomes Gaussian noise-like because of the multiplexing of multi-antenna transmission. Similarly, if some precoding schemes are applied in the MIMO transmitter to raise the capacity or transmission quality, the transmission signal also becomes noise-like. Hence, there is no signal-processing problem in making the transmit signal noise-like by adopting chaos into MIMO systems. If the chaos convolutional code is applied to this MIMO antenna multiplexing, a transmit diversity of MIMO is obtained so that the secure and good bit error rate (BER) performance transmission on physical layer will be achieved.

Manuscript received May 22, 2011.
Manuscript revised November 30, 2011.

[†] The author is with the Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology, Nagoya-shi, 466-8555 Japan.
a) E-mail: okamoto@nitech.ac.jp

DOI: 10.1587/transcom.E95.B.1384

In conventional chaos MIMO schemes, the chaotic multistream schemes have been proposed in [15], [16] where their objectives are securing MIMO and a channel coding effect is not considered. We have proposed a chaos MIMO (C-MIMO) transmission scheme for achieving both the physical-layer security and channel coding gain in [16]. In that study, the performance improvement was confirmed by computer simulations. Enhancing this study, we propose the C-MIMO scheme with considering the performance analysis and a concatenating channel-encoded transmission system. A number of antennas in MIMO systems is usually two or four and the constraint length of chaos coding is terminated at this number. Then, the decoding complexity is restricted in the possible range but the coding gain and physical-layer security are obtained. The new contribution of this paper is to obtain a channel coding effect in chaos MIMO without a transmission efficiency loss.

In the following, the advantage and disadvantage of chaos communication and the system model of the proposed scheme are introduced in Sect. 2. The performance analysis is considered in Sect. 3. Numerical results are shown in Sect. 4 and the conclusions are drawn in Sect. 5.

2. Proposed Chaos MIMO System

2.1 Application of Chaos Modulation

The chaos communication used in this paper is a common key encryption system. In this chaos system, a key information such as initial value of chaos, any parameters of chaos equations is shared only with the target transmitter and receiver. The chaos encryption is processed according to the key in the transmitter. Since the chaos decryption (i.e., chaos decoding) cannot be processed correctly without the common key, the security is ensured. The chaos signals can be quantized into digital signals or unquantized as analog signals. A chaos modulation utilizes this chaos encryption where the chaos signal is modulated by transmit data. The encryption and modulation is jointly conducted and the physical layer security is ensured. However, to obtain the physical layer security each transmit signal is needed to be orthogonal, i.e., the correlation of two signals corresponding to 0 and 1 on GF(2) must be zero. This means one-half Euclidean distance, equivalent to 3 dB penalty, from an inverse correlation pair (e.g., BPSK signals). Since two signals with inverse correlation are an inversion pair of one signal, they are unsecure. Thus, the zero correlation is essential to keep the physical layer security. As described in [9], this degradation of Euclidean distance is the reason why the chaos communication is not widely used. Hence, the advantage of chaos communication is ensuring the physical layer security and the disadvantage is the distance degradation as the cost of encryption. To redeem this degradation, it is necessary for the chaos modulation to compose some channel coding and we proposed a convolutional chaos coded modulation [13]. The bound of coding gain on this scheme is the Shannon limit but it needs long code length and results in unpractical decoding complexity. Thus, in order to reduce the decoding complexity of chaos coded modulation and to obtain the physical layer security and coding gain, we focus on the MIMO multiplexing. When the chaos coding is applied to MIMO multiplexing, a transmit antenna diversity effect is obtained because the transmit data loaded on each antenna are correlated, and more importantly, a number of antenna in MIMO is usually between two and eight, which means the code constraint is limited at this number. This results in a practical decoding complexity. Therefore, the proposed chaos MIMO is effective in terms of channel coding and physical layer security.

Here, we exactly categorize the proposed scheme. In the proposed scheme, the second modulation is conducted to achieve the scrambling and random channel coding, and a chaos is adopted to generate the random signal. Since there is no communication about the key information between the transmitter and receiver during data transmission like [3], the property of *chaos synchronization* [17] is not used and only the sensitivity of the initial value in a chaos signal is utilized in the proposed scheme. However, using chaos as the second modulation enables the variety of key settings. For example, the chaos equation, the chaos modulation scheme, or the chaos iteration number can be treated as the key which is shared by target users [18]. This is discussed in Sect. 2.3. In the next subsection, the system model is introduced.

2.2 System Model

Figure 1 shows the baseband system model of the proposed C-MIMO where N_t and N_r are the numbers of transmit and receive antennas, respectively. In the transmitter, after the channel encoding and the first modulation, the chaos encoding is conducted to MIMO multiplexing signals as a second modulation. This chaos signal is a convolutional coded signal by the transmit data. In the receiver, a joint maximum likelihood decoding (MLD) of the chaos decoding and the MIMO detection is conducted. As shown in the figure, the proposed system is basically the same as conventional MIMO multiplexing system except the multiplication of chaos symbols at the 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

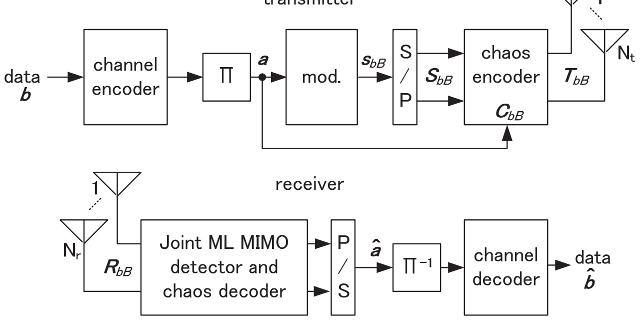


Fig. 1 Block diagram of chaos MIMO system.

this block unit. Let the information bit in the block as b_m $(1 \leq m \leq M)$ and the transmission bit in the block after channel coding and interleaving as $a_n(1 \leq n \leq N)$ where M and N are the number of information bits and transmission bits in one block, respectively. Then, when the number of modulation points is $Q = 2^q$, the number of transmission symbols in the block becomes N/q. Hereafter, this block is defined as 'one code block'. In this paper, BPSK (q=1) and QPSK (q=2) modulations are considered as the first modulation. The modulated symbols are serial-to-parallel transformed and loaded to each antenna where the transmit MIMO vector consisting of N_t symbols is composed. Then, using B MIMO vectors, the chaos encoding is conducted as the second modulation. This B MIMO vectors are defined as 'one MIMO block'. One code block has $N/(qBN_t)$ MIMO blocks and when the number of the MIMO blocks is labeled as b_B, its range becomes $0 \leq b_B \leq N/(qBN_t) - 1$. The numbers of transmit symbols and bits in one MIMO block become BN_t and qBN_t, respectively. Let k of $0 \leq k \leq B-1$ as the time index in one MIMO block and then, the transmit vector at time k in MIMO b_B block is given by

$$\boldsymbol{s}_{b_B}(k) = [s_1(k) \cdots s_{N_t}(k)]^T$$

where $s_i(k)$ is the transmit symbol from antenna $i(1 \leq i \leq N_t)$. The $(N_t \times B)$-transmit MIMO block matrix becomes

$$\boldsymbol{S}_{b_B} = [\boldsymbol{s}_{b_B}(0) \cdots \boldsymbol{s}_{b_B}(B-1)]$$

Then, this transmit block is second-modulated (encrypted) by a chaos encoding matrix $\boldsymbol{C}_{bB}$ as follows.

$$\boldsymbol{T}_{b_B} = \boldsymbol{C}_{b_B} \circ \boldsymbol{S}_{b_B} = [\boldsymbol{t}_{b_B}(0) \cdots \boldsymbol{t}_{b_B}(B-1)] \tag{1}$$

Here, $\circ$ means the scalar product (Hadamard product) and $\boldsymbol{T}_{bB}$ is the encoded MIMO block to be transmitted where each vector is composed by

$$\boldsymbol{t}_{b_B}(k) = [t_1(k) \cdots t_{N_t}(k)]^T$$

The $(N_t \times B)$-chaos matrix is described by

$$\boldsymbol{C}_{b_B} = \begin{bmatrix} c_{b_B}(1) & \cdots & c_{b_B}(\{B-1\}N_t+1) \\ \vdots & \ddots & \vdots \\ c_{b_B}(N_t) & \cdots & c_{b_B}(BN_t) \end{bmatrix} \tag{2}$$

Finally, $\boldsymbol{T}_{bB}$ is transmitted. The generation of chaos matrix $\boldsymbol{C}_{bB}$ is described in the next subsection. This multiplication is the same as a space-time block coding (STBC) without loss of transmission efficiency. That is, a MIMO multi-stream transmission and coding are achieved. It is assumed that the MIMO channel is an i.i.d. flat fading between every antenna. The $(N_r \times N_t)$-MIMO channel matrix is given by

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

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

$$\boldsymbol{R}_{b_B} = [\boldsymbol{r}_{b_B}(0) \cdots \boldsymbol{r}_{b_B}(B-1)]$$
$$\boldsymbol{r}_{b_B}(k) = [r_1(k) \cdots r_{N_r}(k)]^T$$

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

$$\boldsymbol{N}_{b_B}(k) = [\boldsymbol{n}_{b_B}(0) \cdots \boldsymbol{n}_{b_B}(B-1)]$$
$$\boldsymbol{n}_{b_B}(k) = [n_1(k) \cdots n_{N_r}(k)]^T$$

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

$$\boldsymbol{r}_{b_B}(k) = \boldsymbol{H}_{b_B}(k)\boldsymbol{t}_{b_B}(k) + \boldsymbol{n}_{b_B}(k) \tag{3}$$

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

$$\hat{\boldsymbol{a}}_{b_B} = \arg\min_{\boldsymbol{a}_{bB}} \left\| \boldsymbol{R}_{b_B} - \boldsymbol{H}_{b_B} \boldsymbol{T}_{b_B} \right\|_F^2 \tag{4}$$

where the matrices and the vector are given by

$$\boldsymbol{H}_{b_B} = [\boldsymbol{H}_{b_B}(0) \cdots \boldsymbol{H}_{b_B}(B-1)]$$

$$\boldsymbol{T}_{b_B} = \begin{bmatrix} \boldsymbol{t}_{b_B}(0) & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{t}_{b_B}(1) & & \\ \vdots & & \ddots & \vdots \\ \boldsymbol{0} & \cdots & & \boldsymbol{t}_{b_B}(B-1) \end{bmatrix}$$

$$\hat{\boldsymbol{a}}_{b_B} = \left\{\hat{a}_i \cdots \hat{a}_{i+qBN_t-1}\right\}, \boldsymbol{a}_{b_B} = \left\{a_i \cdots a_{i+qBN_t-1}\right\}$$
$$(i = b_B qBN_t + 1)$$

and $\|\cdot\|_F$ is the Frobenius norm. Since this is the MLD for one MIMO block, the number of decoding search becomes 2^{qBN_t}. After decoding $\hat{a}_n$ $(1 \leq n \leq N)$ of all MIMO blocks, the de-interleaving is done and $\hat{b}_m$ $(1 \leq m \leq M)$ is decoded by a hard-decision decoding of the outer channel code.

In addition, the joint ML for outer concatenated channel coding can be composed. Figure 2 shows the block diagram of C-MIMO in the case of joint MIMO detection with chaos and channel decoding using soft-decision Viterbi algorithm. To construct the joint trellis diagram of the channel encoding and the chaos encoding, the interleaver cannot be inserted. The MIMO detection, chaos and channel decoding are simultaneously conducted by Viterbi algorithm for the

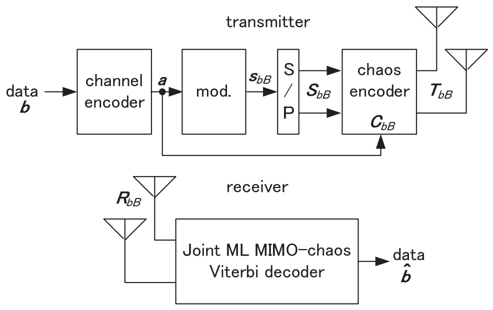


Fig. 2 System block diagram of chaos MIMO with joint ML Viterbi decoding.

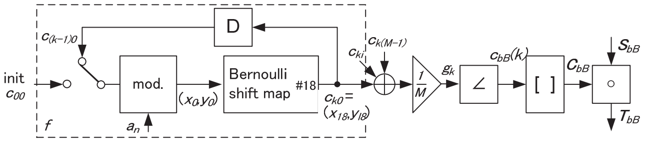


Fig. 3 Block diagram of chaos encoder.

joint trellis diagram. Specifically, the MLD is conducted for receive MIMO vector of (3) by

$$\hat{\boldsymbol{b}} = \arg\min_{b} \sum_{b_B=0}^{N/(qBN_t)-1} \left\| \boldsymbol{R}_{b_B} - \boldsymbol{H}_{b_B} \boldsymbol{T}_{b_B} \right\|_F^2$$

where $\hat{\boldsymbol{b}}$ is the all information bits in one code block.

2.3 Configuration of Second Chaos Modulation

In the proposed scheme, the transmit MIMO block $\boldsymbol{s}_{b_B}(k)$ is second-modulated by the encoded chaos signals as shown in (1). This can be regarded as a rate−1 coded modulation and this chaos coded modulation enables the security and channel coding gain. Figure 3 shows the block diagram of the chaos encoder. M independent chaos signals are encoded by a transmit bit and a Gaussian noise vector is generated by averaging the M chaos signals. Using the phase of its noise vector the encoding chaos matrix $\boldsymbol{C}_{bB}$ is composed. First, it is assumed that the transmitter and receiver have the identical Mchaos initial symbols of

$$\begin{aligned} &\boldsymbol{c}(0) = [c_{00} \cdots c_{0(M-1)}], \quad c_{ki} \in \mathbb{C}, \\ &0 < \mathrm{Re}[c_{0i}], \mathrm{Im}[c_{0i}] < 1 \end{aligned} \tag{5}$$

This vector is the key signal of encryption and the proposed scheme is categorized as the common key encryption. The condition of this key signal is that they are identical at the transmitter and the receiver to obtain the synchronization of chaos. To avoid a similar transmission signal pattern, it is desirable to scramble the key signal by some pseudo random periodic signals such as PN codes on every MIMO block. At time of k=1, this initial chaos is modulated by the transmit bit as follows

$$x_0 = \begin{cases} \mathrm{Re}[c_{(k-1)i}] & a_{k1}=0 \\ 1-\mathrm{Re}[c_{(k-1)i}] & a_{k1}=1, \mathrm{Re}[c_{(k-1)i}] > 1/2 \\ \mathrm{Re}[c_{(k-1)i}]+1/2 & a_{k1}=1, \mathrm{Re}[c_{(k-1)i}] \leq 1/2 \end{cases} \tag{6}$$

where x_0 is the real part of $c_{0i} = x_0 + jy_0$ and a_{ki} is a bitwise right shift of transmit bit sequence $\boldsymbol{a}_{b_B}$ in MIMO block. It is given by

$$\begin{aligned} &a_{ki} = a_n \\ &n=[\{qN_t(B+k-1)+i-2\} \bmod (qBN_t)]+b_B qBN_t+1 \end{aligned} \tag{7}$$

In BPSK modulation at the first modulation, y_0 is not modulated as of (6) because only a_{k1} is transmitted at time k, while in QPSK modulation y_0 is modulated similarly by (6) using a_{k2}. Then, the chaos signal is processed by

$$x_{l+1} = 2x_l \bmod 1, \quad y_{l+1} = 2y_l \bmod 1$$

This is the Bernoulli shift map transition [8]. The chaos signal at time k is calculated by

$$c_{ki} = x_{18} + jy_{18}$$

and this operation is conducted for all M chaos signals c_{ki} $(0 \leq i \leq M-1)$. Using the calculated c_{ki}, the pseudo-Gaussian noise signal g_k is generated by averaging as follows.

$$\begin{aligned} g_k = \frac{1}{M} \sum_{i=0}^{M-1} &\{(\mathrm{Re}[c_{ki}] + \mathrm{Im}[c_{ki}]) \exp(j8\pi[\mathrm{Re}[c_{ki}] \\ &- \mathrm{Im}[c_{ki}]])\} \quad 1 \leq k \leq BN_t \end{aligned}$$

Here, M is the number of independent chaos signals used for making white noise by central limit theorem, and is set to relatively large value more than five. Finally, the unit vector is generated by g_k as follows

$$c_{b_B}(k) = \exp\left\{ j2\pi \tan^{-1} (\mathrm{Im}[g_k]/\mathrm{Re}[g_k]) \right\}$$

and this $c_{b_B}(k)$ is used as the second-modulating symbol as shown in (2). Hence, the second modulation is limited to a phase shift by using the complex unit vector $c_{b_B}(k)$ and the power of transmit signal is unchanged. The above operation is iterated for $1 \leq k \leq BN_t$ and the chaos matrix $\boldsymbol{C}_{bB}$ is calculated. In general expression, this chaos vector at time k is described by

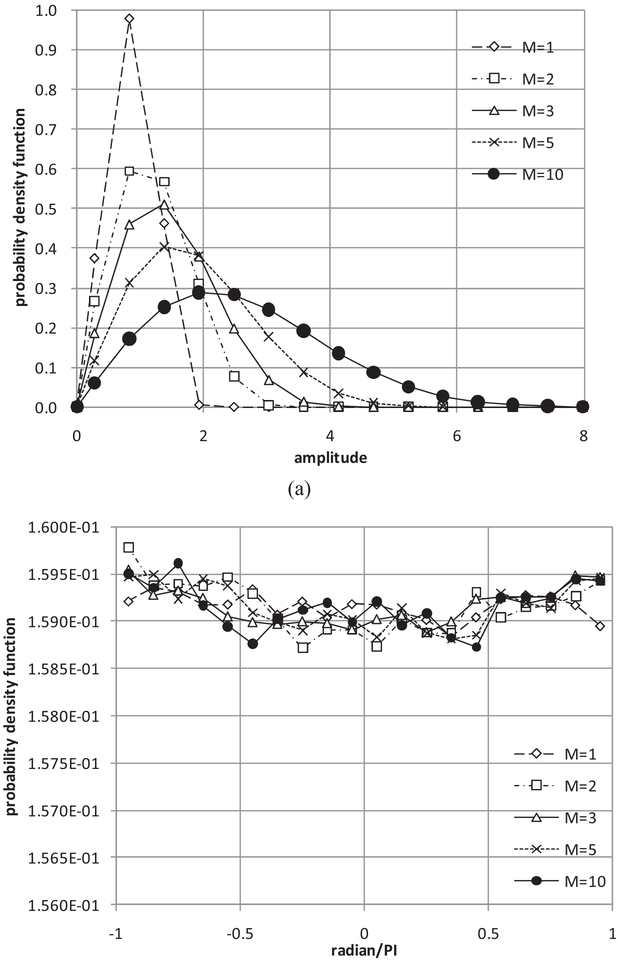
$$\begin{aligned} &\boldsymbol{c}_{b_B}(k) = [c_{k0} \cdots c_{k(M-1)}], \quad c_{ki} \in \mathbb{C}, \\ &0 < \mathrm{Re}[c_{ki}], \mathrm{Im}[c_{ki}] < 1 \end{aligned}$$

and the chaos processing is given by the chaos convolution of

$$\boldsymbol{c}_{b_B}(k) = f\left(\boldsymbol{c}_{b_B}(k-1), a_{k1}, \cdots, a_{kq}\right)$$

Then, the pseudo-noise signal g_k is generated and the element $c_{b_B}(k)$ of chaos matrix is calculated by extracting its phase information.

A dominant factor of channel coding of this chaos second modulation is the same as the dominant factor of conventional channel coding, that is, the degree of transmitting bit correlation into the encoded sequence, and the closeness to a random coding. In the proposed scheme, the bit correlation effect is raised by the right cyclic shift in MIMO block as shown in (7) under the constraint of unit encoding vector for constant transmit power, resulting in a larger coding gain. In addition, the random coding is achieved by using M independent chaos signals. To confirm it, the probability density function (pdf) of chaotic pseudo-Gaussian noise signal g_k is calculated as shown in Fig. 4. It is confirmed that the pdfs of the amplitude and phase converge on Rayleigh and uniform distribution, respectively, due to the central limit theorem. From a point of view of the random coding in a complex plane, the phase distribution should be perfectly uniform to $1/(2\pi)$ to obtain the best performance. However, since it was difficult to obtain the ideal distribution using chaos with information embedding, the pdf of Fig. 4(b) is



(a)

(b)

Fig. 4 Normalized probability density function of pseudo random signal g_k; (a) amplitude distribution, and (b) phase distribution.

regarded as a uniform. It is found that M=5 is sufficient to obtain the complex Gaussian distribution on g_k of baseband vector. M=10 is used in the following consideration.

In principle, the configuration of chaos, such as chaos equation, modulation setting, or chaos transition, can be freely changed other than that of this subsection whenever the random coding condition is satisfied. The configuration in this paper is determined by a heuristic search. Furthermore, it is also possible that if this configuration is changed for each transmission pair, the configuration itself can be treated as the common key which only the transmitter and receiver knows.

Here, a linear nulling scheme of inverse matrix multiplication exists for MIMO detection other than MLD as a popular low complexity scheme. However, since the chaos block coding is applied as shown in (1) in the proposed scheme, the symbol-by-symbol detection and decoding cannot be utilized and the sequential decoding of (4) 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.

3. Performance Analysis of C-MIMO

3.1 Asymptotic Characteristic of Bit Error Rate

It is assumed that the channel is a flat fading in ($N_t \times N_r$)-MIMO transmission and is perfectly known to the receiver. Then, the asymptotic BER characteristic of MIMO-MLD in relatively higher SNR region is given by

$$P_{b,\mathrm{asymp}} = \frac{\alpha}{q}\left(\frac{N_r}{2q\gamma_b}\right)^{N_r}\binom{2N_r - 1}{N_r}$$

where q is the number of transmit bits per symbol at one antenna and γ_b is E_b/N_0 per receive antenna [19]. α is a sum of squared Euclidean distances between two vectors given by

$$\alpha = Q^{-N_t}\sum_m\sum_j\sum_i a_{s_m,ij}^{-N_r}$$
$$a_{s_m,ij} = \left\|\boldsymbol{d}_i - \boldsymbol{d}_j\right\|^2/(2E_s) \tag{8}$$

where $\{\boldsymbol{d}\}$ is a set of Q^{N_t} transmit vectors, $\{S_m\}$ is a set of Q modulation points, $\left\{\boldsymbol{d}_j\right\}$ is the subset of Q^{Nt-1} transmit vectors whose k-th symbol is S_m ($1 \le j \le Q^{N_t-1}$), and $\{\boldsymbol{d}_i\}$ is the complementary subset of ($\mathrm{Q}^{Nt} - \mathrm{Q}^{Nt-1}$) transmit vectors whose k-th symbol is not S_m. Since the actual transmit symbol of C-MIMO $t_i(k)$ is a constant-amplitude and random-phase symbol as described in Sect. 2.2, the Euclidean distance in (8) also becomes random regardless to the combination of $\boldsymbol{d}_j$ and $\boldsymbol{d}_i$. However, since the Euclidean distance in (8) is the amplitude of the difference between two random and constant-amplitude symbols, its expectation value becomes constant. Then, we assume it as the constant value of $\left\|\boldsymbol{d}_i - \boldsymbol{d}_j\right\|^2 = E\left[d^2\right] = \overline{d^2}$. Considering that the length of C-MIMO vector is B due to the block-wise chaos encoding, the squared Euclidean distance of (8) becomes

$$a_{s_m,ij} = \overline{d^2}B/(2E_s)$$

Unfortunately, this $\overline{d^2}$ is hardly derived theoretically because the operation of the chaos encoding is chaotic nonlinear signal processing, which is hard to predict.

Therefore, we calculate it numerically. Table 1 shows the normalized squared Euclidean distance of C-MIMO when the first modulation is BPSK or QPSK. Compared with the distance of conventional BPSK of 4, the proposed scheme with BPSK has almost a half distance of 2. This is caused by the chaotic random coding with a phase rotation, which is a cost of encryption on the physical-layer as described in Sect. 2.1. To redeem it the coding gain is obtained by the block coding of B ($\geq$ 2) in C-MIMO. From Table 1, it is expected that the BER performance of the proposed scheme will overcome at $B \geq 2$ for the conventional MIMO-MLD because the squared Euclidean distances of the MIMO-MLD are 4 with BPSK and 2 with QPSK. It is

Table 1 Normalized squared Euclidean distance per one symbol of C-MIMO.

modulation	N_t	B	$\overline{d^2}/E_s$
BPSK	2	2	2.13
	2	3	2.03
	4	2	2.01
QPSK	2	2	1.001
	4	3	1.0005

Table 2 Comparison of decoding complexity.

	Proposed	Conventional
System	C-MIMO-MLD	MIMO-MLD
Uncoded, or non-systematic code (NSC) with sequencial decoding	2^{qBN_t}	2^{qN_t}
Non-systematic code (NSC) with joint decoding	$2^{\max(qBN_t,K_c)}L$	$2^{\max(qN_t,K_c)}L$

confirmed in Sect. 4.

3.2 Decoding Complexity

Table 2 shows the comparison of decoding complexity between the proposed scheme and the conventional MIMO-MLD, where K_c is the constraint length of the outer convolutional code. Here, the calculation complexity is defined as the number of decoding searches. The proposed scheme needs 2^B-times extra calculation compared with the conventional scheme in non-outer coding system or in the sequential decoding system as shown in Fig. 1. In the joint Viterbi decoding system 2^B-times calculation is needed, too when $K_c < qN_t$ is satisfied. Therefore, the proposed scheme needs an extra calculation due to the B-block MLD processing and it depends on the number of transmit bits q and the number of transmit antenna N_t.

4. Numerical Results

The performances of the proposed scheme are evaluated by computer simulations where the simulation conditions are listed in Table 3. It is assumed that thechannel is symbol i.i.d. or MIMO-block i.i.d. quasi-static Rayleigh fading between any transmit and receive antennas, and that the channel is perfectly known to the receiver. This symbol i.i.d. assumption will be satisfied by some additional interleavers between the chaos encoder and MIMO antennas in Figs. 1 and 2. It is also assumed that the initial chaos is synchronized between the transmitter and receiver. To obtain the average performance, the initial key vector of (5) is randomly changed at every block in this simulation. As a concatenation code outside of Fig. 1, no coding case and the convolutional coding (CC) case with the memory length K_c=2 and code length L=200 are considered. In decoding, (4) is conducted in the uncoded case and the Euclidean distance-based Viterbi decoding where all combinations of C-MIMO-MLD correspond to each state of trellis diagram is conducted in the convolutional coding case. As the conventional scheme, the performance of MIMO-MLD is compared.

Table 3 Simulation conditions.

Modulation	BPSK(q=1), QPSK(q=2)
Num. of antenna	Nt=Nr=2,4
Num. of MIMO symbols on 1 block	B=2,3,4,5
Chaos	Bernoulli shift map
Num. of chaos signals	M=10
Initial chaos sync.	perfect
Channel	symbol i.i.d. or block i.i.d quasi-static flat Rayleigh fading
Receive channel state inf. (CSI)	perfect
Outer channel coding	uncoded
	convolutional code NSC[7 5], rate=1/2, L=200 Kc=2, Viterbi decoding

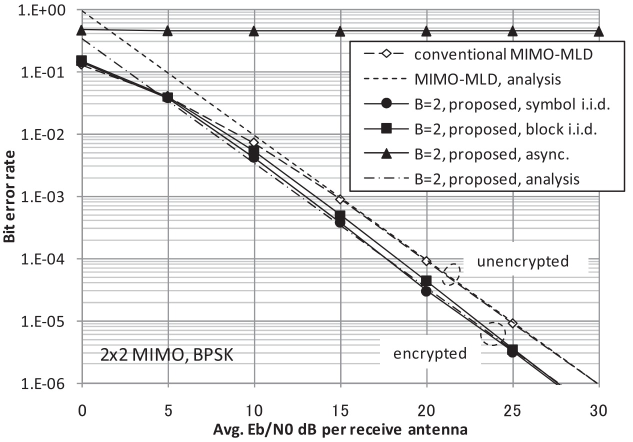


Fig. 5 BER performances with $N_t = N_r = 2$, $B = 2$ and BPSK without outer code.

4.1 Performance Comparison without Concatenated Code

Figures 5 and 6 show the BER performance versus E_b/N_0 with BPSK modulation, $N_t = N_r$=2, and the block length B=2 and 3. Hereafter, the channel is assumed as symbol i.i.d. for the conventional MIMO-MLD. Compared with the unencrypted MIMO-MLD the coding gains of BPSK with B=2 and 3 are 2.5 dB and 3.5 dB, respectively, at BER of 10^{-5}. This is the effect of rate−1 chaos encoding. The analytical curve and the simulation performance asymptotically coincide at higher SNR region, and it is shown that the assumption of 3.1 is valid. For two channel scenarios, naturally the performance in symbol i.i.d. channel is somewhat better than that of block fading channel because of a time-diversity effect. The BER of the case that M-initial key symbols are 10^{-3} different from those of transmitter is almost 0.5, which means the transmit data cannot be decoded cor-

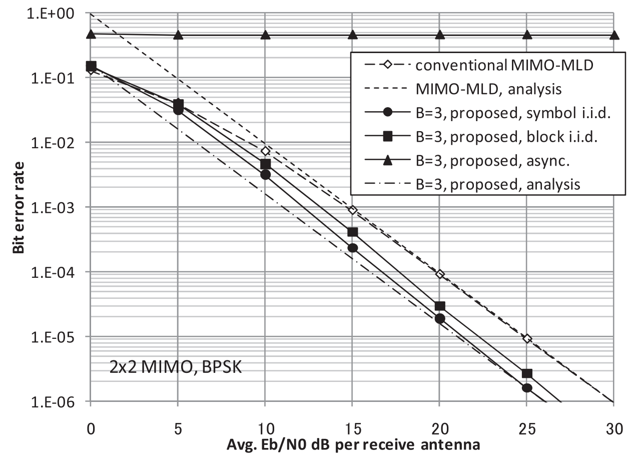


Fig. 6 BER performances with $N_t = N_r = 2$, $B = 3$ and BPSK without outer code.

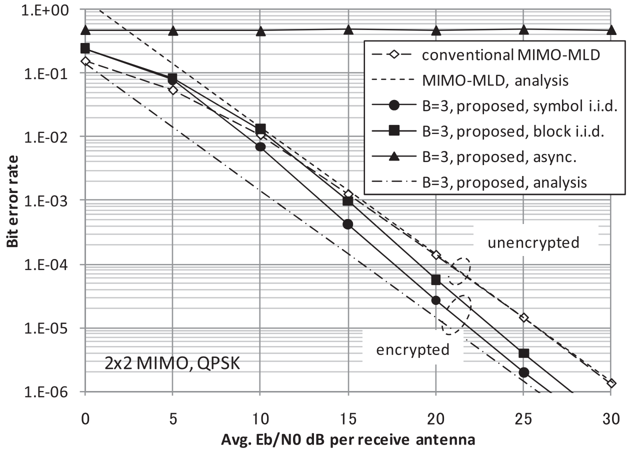


Fig. 8 BER performances with $N_t = N_r = 2$, $B = 3$ and QPSK without outer code.

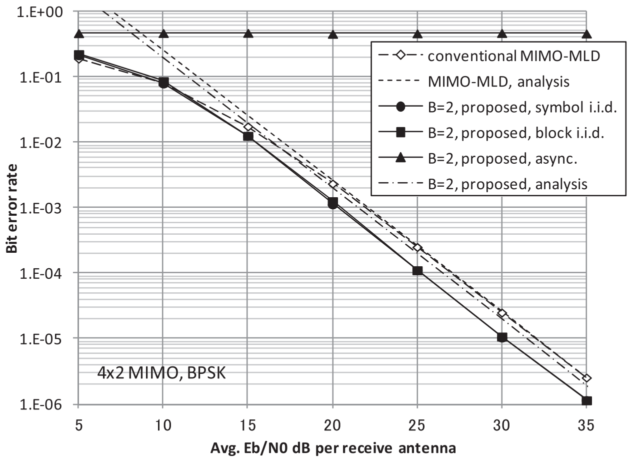


Fig. 7 BER performances with $N_t = 4$, $N_r = 2$, $B = 2$ and BPSK without outer code.

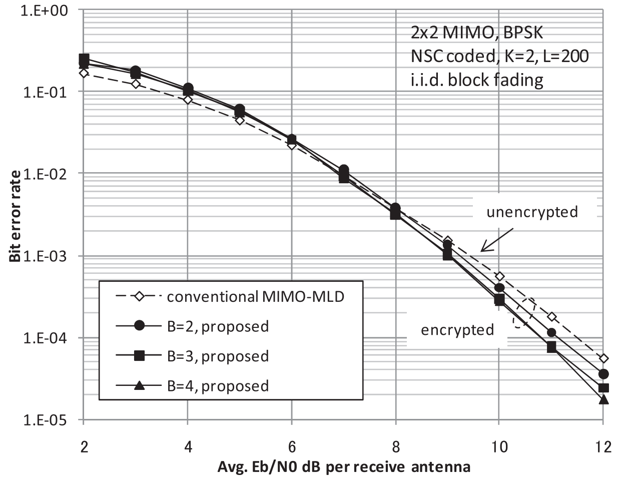


Fig. 9 BER performances of concatenated code with sequential decoding, $N_t = N_r = 2$, $B = 2$ to 4 and BPSK.

rectly even if the difference of the key in (5) is very small and the physical layer security is ensured.

Next, Fig. 7 shows the BER of N_t=4, N_r=2 and BPSK. The performance improvement is kept as 1.7 dB gain with B=2 at BER of 10^{-5}. Similarly, as shown in Fig. 8, the BERs of QPSK with B=2 and 3 have 1.1 dB and 3.1 dB gains, respectively, at BER of 10^{-5}.

Hence, the transmit antenna diversity and coding gain are obtained by chaos coding compared with the conventional MIMO multiplexing. Since the Euclidean distance becomes half by the chaos modulation as described in Sect. 2, the performance improvement is obtained with B=2, i.e., by utilizing the longer chaos code length and its time diversity effect of fading in symbol i.i.d. case. Numerical results showed that the sufficient effect was obtained with B=2. The proposed scheme has the physical layer security and coding gain which the conventional scheme doesn't have. When the transmit antenna N_t increases, a larger gain will be obtained by the transmit antenna diversity effect. However, as shown in Table 1, the squared Euclidean distance is decreased at N_t=4, and then, the coding gain was decreased.

4.2 Performance Comparison with Concatenated Code

Next, the performances with an outer concatenated channel code are evaluated. The BER performance of the system in Fig. 1 with the sequential hard-decision decoding is shown in Fig. 9 where $N_t = N_r = 2$ and $B = 2$ to 4. From the results, all performances are improved from the uncoded system and the proposed scheme has better performances from B=2, which is obvious because of the uncoded results of Figs. 5 and 6. With B=4, the 0.7-dB chaos coding gain is obtained at BER of 10^{-4}. Hence, it is shown that the proposed scheme is still effective in the coding system.

Finally, the performance of joint decoding as shown in Fig. 2 is calculated. Compared with the sequential decoding of Fig. 9, the results of Fig. 10 show the improved performances because of the joint soft-decision MLD. However, in the block fading channel, the proposed scheme has worse

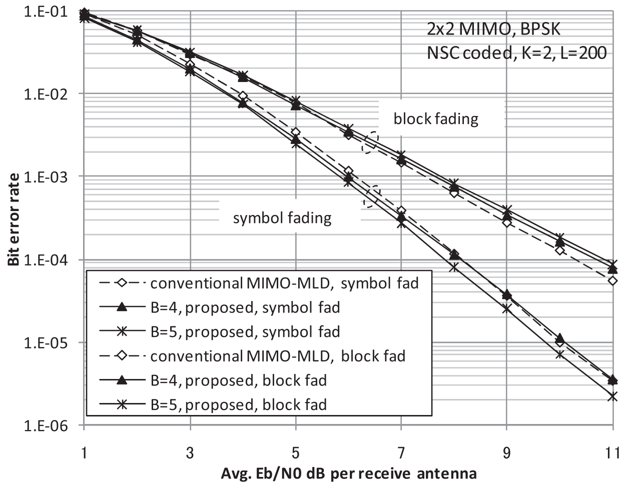


Fig. 10 BER performances of concatenated code with joint Viterbi decoding, $N_t = N_r = 2$, $B = 4, 5$ and BPSK.

performances due to the lack of interleaver between outer code and C-MIMO. On the contrary, the proposed scheme outperforms the conventional scheme in the symbol i.i.d. fading channel. If the MIMO block length is longer than the code-constraint length of the outer code, say $B \geq 4$, the chaos-coding gain is obtained. The same BER as the conventional MIMO-MLD was obtained with $B < 4$, it was not drawn in Fig. 10 though. The 0.46 dB coding gains are obtained at BER of 10^{-5} with B=5. Since the chaos coding length is longer than the CC constraint length, the minimum error event path of CC is effectively corrected by the chaos code. Thus, even in channel coding systems, the proposed scheme can obtain the performance improvement with $B > K_c + 1$. Note that if the decoding scheme of outer code is hard-decision type as shown in Fig. 1, this constraint length condition is released and the chaos-coding gain is obtained from B=2 as shown in Fig. 9. The combined MLD is needed when the soft-decision decoding is adopted as this example. It is expected that a serial-concatenated iterative component decoding with log-likelihood ratio (LLR) such as turbo codes can be adopted for C-MIMO. This will be considered in future studies.

Consequently, regardless of the existence of the outer concatenation code, the proposed scheme has the property of a physical-layer security and a coding gain by the convolutional encoding of chaos into the MIMO antenna multiplexing.

5. Conclusions

In this paper, we proposed a chaos MIMO transmission scheme achieving high-quality, large capacity, and secure communication on physical layer by adopting the chaos coding into MIMO multiplexing. The performance improvement was confirmed by the asymptotical performance analysis and the simulation results. We showed that the coding gain and physical layer security were obtained in tradeoff with decoding complexity increase and the block length of B=2 was sufficient in this simulation. In the condition of BPSK, B=2, and N_t=2, the numbers of ML decoding search in the conventional and the proposed schemes are 4 and 16, respectively, which is 4 times of conventional scheme. This complexity increase is acceptable. In the proposed scheme, only a chaos multiplication to each MIMO transmit symbols is needed, which is a little additional mechanism. Similarly, only the MLD with chaos is needed in the receiver. Thus, the implementation of the proposed scheme to MIMO system is relatively straightforward. This C-MIMO scheme is useful for achieving the physical-layer security.

Acknowledgments

This research was partially supported by KDDI foundation. The author wishes to thank for their support.

References

[1] M.E. Hellman, "An overview of public key cryptography," IEEE Commun. Mag., vol.16, no.6, pp.24–32, Nov. 1978.

[2] V. Manral, "Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH)," RFC 4835, IETF, April 2007.

[3] T.L. Carroll and L.M. Pecora, "Synchronizing chaotic circuits," IEEE Trans. Circuit Syst., vol.38, no.4, pp.453–456, April 1991.

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

[5] T. Yang, "A survey of chaotic secure communication systems," Int. J. Comp. Cognition, vol.2, pp.81–130, June 2004.

[6] 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. Circuit Syst., vol.40, no.10, pp.634–641, Oct. 1993.

[7] G. Kolumban and M.P. Kennedy, "Recent results for chaotic modulation schemes," Proc. IEEE Intl. Symp. on Circuit Syst., vol.3, pp.141–144, May 2001.

[8] B. Chen and G.W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," IEEE Trans. Commun., vol.46, no.7, pp.881–890, July 1998.

[9] S. Kozic, T. Schimming, and M. Hasler, "Controlled one- and multi-dimensional modulations using chaotic maps," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol.53, no.9, pp.2048–2059, 2006.

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

[11] F.J. Escribano, S. Kozic, L. López, M.A. F. Sanjuán, and M. Hasler, "Turbo-like structures for chaos encoding and decoding," IEEE Trans. Commun., vol.57, no.3, pp.597–601, March 2009.

[12] F.J. Escribano, L. López, and M.A.F. Sanjuán, "Exploiting symbolic dynamics in chaos coded communications with maximum a posteriori algorithm," Electron. Lett., vol.42, no.17, pp.984–986, Aug. 2006.

[13] E. Okamoto and Y. Iwanami, "A trellis-coded chaotic modulation scheme," Proc. IEEE Int'l Conf. Commun., vol.11, pp.5010–5015, June 2006.

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

[15] G. Zheng, D. Boutat, T. Floquet, and J.-P. Barbot, "Secure communication based on multi-input multi-output, chaotic system with large message amplitude," Chaos, Solitons & Fractals, vol.41, no.3, pp.1510–1517, 2009.

[16] E. Okamoto, "A chaos MIMO transmission scheme for secure communications on physical layer," Proc. IEEE Vehicular Technology Conf. (VTC2011-Spring), May 2011.

[17] M. Wada, J. Kawata, Y. Nisiho, and A. Ushida, "BER estimation of a chaos communication system including modulatoin-demodulation circuits," IEICE Trans. Fundamentals, vol.E83-A, no.3, pp.563–566, March 2000.

[18] E. Okamoto, "A comparative study of bit error rate performance in chaos MIMO transmission system," Proc. Int'l Sym. on Nonlinear Theory and its Applications (NOLTA), pp.33–36, Sept. 2011.

[19] X. Zhu and R.D. Murch, "Performance analysis of maximum likelihood detection in a MIMO antenna system," IEEE Trans. Commun., vol.50, no.2, pp.187–191, Feb. 2002.

Eiji Okamoto received the B.E., M.S., and Ph.D. degrees in Electrical Engineering from Kyoto University in 1993, 1995, and 2003, respectively. In 1995 he joined the Communications Research Laboratory (CRL), Japan. Currently, he is an associate professor at Nagoya Institute of Technology. In 2004 he was a guest researcher at Simon Fraser University. He received the Young Researchers' Award in 1999, Communications Society: Distinguished Contributions Award in 2005, 2007, and 2010 from IEICE, the FUNAI Information Technology Award for Young Researchers in 2008, the Best Student Paper Award in AIAA International Communications Satellite Systems Conference (ICSSC) in 2011, and the Excellent Paper Award in International Conference on Information Networking (ICOIN) in 2012. His current research interests are in the areas of wireless technologies, satellite communication, and mobile communication systems. He is a member of IEEE.