Performance improvement of chaos MIMO scheme using advanced stochastic characteristics

Eiji Okamoto1a) and Naoto Horiike1

1 Graduate School of Engineering, Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan
a) okamoto@nitech.ac.jp

Abstract:
Chaos multiple-input multiple-output (C-MIMO) is a transmission scheme that uses Gaussian signal transmission based on chaos, where physical-layer security and channel coding effect are obtained. However, because the Gaussian signals are generated according to the principle of central limit theorem, about ten independent chaos signals are needed, resulting in increased calculation complexity. In addition, the probability density function of the phase of transmit signals slightly deviates from uniform distribution, which degrades the bit error rate (BER) performance. Therefore, we propose a C-MIMO scheme with improved Gaussian modulation, in which the stochastic characteristic is improved by applying the Box–Muller method with only one chaos signal.

Keywords: chaos communication, MIMO, Gaussian modulation, Box–Muller method, central limit theorem.

Classification: Wireless communication technologies

References


1 Introduction

One of the key technologies for currently available higher capacity wireless communication systems is multiple-input multiple-output (MIMO) transmission, which is a mandatory condition for Long-Term Evolution system and later. In addition, physical-layer security that assures wireless security has attracted attention. We propose a chaos MIMO (C-MIMO) transmission scheme in which channel coding effect and physical-layer security are obtained to satisfy both abovementioned requirements [1]. In C-MIMO, a Gaussian transmit signal correlated to a transmit bit sequence is composed of the chaos modulated signals. Then, common key encryption, where the key is the initial values of chaos, and channel coding by Gaussian coded modulation are realized. In the receiver, decryption and decoding are carried out simultaneously using maximum likelihood sequence estimation (MLSE) decoding.

In the conventional scheme in [1], according to the principle of central limit theorem, about ten independent chaos signals with different initial values are prepared, and the Gaussian distribution is obtained by averaging them. However, because of the use of ten chaos signals, the calculation complexity for preparing transmission signals increases. In addition, the probability density function (PDF) of the phase of transmit signals deviates slightly from uniform distribution, and this degrades the bit error rate (BER) performance.

Therefore, we propose a C-MIMO scheme with improved Gaussian modulation, in which the stochastic characteristic, particularly the phase characteristic, is improved by applying the Box–Muller method [2] with only one chaos signal. This enhances the channel coding effect. Furthermore, as the number of chaos sequences is reduced to one, the calculation complexity involved in generating the Gaussian signals is reduced. The improvement in performance is shown through numerical simulations.

2 Chaos MIMO transmission system

Fig. 1 shows the system model of C-MIMO with an outer channel encoder in the transmitter and a turbo decoder that uses log-likelihood ratio (LLR) in the receiver [1]. A K-bit transmit sequence \( u = \{u_0, L, u_{K-1}\} \), \( u_i \in \{0,1\} \) is encoded, and we obtain an N-bit \( (N > K) \) sequence \( u' = \{u'_0, L, u'_{N-1}\} \), \( u'_i \in \{0,1\} \). Next, \( u' \) is interleaved to the sequence \( b = \{b_0, L, b_{N-1}\} \). Then, \( b \) is divided by \( NB \) bit, and it is block...
modulated with block length $B$ by the C-MIMO scheme with 1-bit/symbol/antenna transmission efficiency, where $N_t$ is the number of transmit antennas. Using this block modulation, the C-MIMO scheme can realize channel-coding gain without decreasing rate efficiency. Let $b_n = \{b_{n,0}, \ldots, b_{n,N_tB-1}\}$ be the $n$-th transmit bit sequence of the $n$-th C-MIMO block ( $0 \leq n \leq (N_t/N_tB)-1$ ). $b_n$ is chaos-modulated, and a complex Gaussian symbol sequence $s_n = \{s_{n,0}, \ldots, s_{n,N_tB-1}\}$ is obtained (described in Section 2.1). Then, $s_n$ is transmitted by the MIMO multiplexing transmission scheme $B$ times for every $N_t$ symbol. The MIMO transmit vector $s_n(k)$ at time $k$ ($0 \leq k \leq B-1$) is described by

$$s_n(k) = \{s(k,0), \ldots, s(N_t-1, k)\}^T = \{s_{n,kN_t}, \ldots, s_{n,(k+1)N_t-1}\}^T,$$

where $s_i(k)$ is the transmit symbol from the $i$-th antenna ($1 \leq i \leq N_t$ ) at time $k$, and $T$ denotes the transpose. Then, one transmit block is described by $S_{B,n} = \{s_n(0), \ldots, s_n(B-1)\}$.

In the receiver, the LLR-based MLSE is conducted for each C-MIMO block, and iterative turbo decoding between the C-MIMO decoder and the outer decoder is utilized [1]. The details are omitted here due to space limitations.

### 2.1 Proposed chaos modulation based on Box–Muller method

The proposed chaos modulation scheme that generates $S_{B,n}$ from $b_n$ is introduced in this section. This scheme is a common-key encryption, and the key signal that is shared between the transmitter and the receiver is set as

$$c_{i0} = 0, \quad 0 < \text{Re}(c_{i0}) < 1, \quad 0 < \text{Im}(c_{i0}) < 1,$$

where $c_{i0}$ is a random complex symbol and is used as the initial value of the chaotic system. For practical systems, the key of (1) can be generated and shared using a specific ID, such as the pre-installed hardware identifier of the transmitter or receiver. In this study, it is assumed that the key is shared by the transmitter and receiver. The real and imaginary parts of $c_{i-1,0}$ are modulated by the different bits of $b_{n,i}$ as

$$x_0 = \begin{cases} a & (b_{n,m} = 0) \\ 1-a & (b_{n,m} = 1, a > 1/2) \\ a + 1/2 & (b_{n,m} = 1, a \leq 1/2) \end{cases},$$

Real part: $a = \text{Re}(c_{i-1,0})$, $m = i - 1$

Imaginary part: $a = \text{Im}(c_{i-1,0})$, $m = i \mod (N_tB)$

in the range $1 \leq i \leq N_tB$. When $i = 1$, the initial key signal is modulated. Then, the variable $x_0$ is processed by the Bernoulli shift map as

$$x_{i+1} = 2x_i \mod 1, \quad 0 \leq i \leq Ite-1,$$

where $Ite$ is the chaos iteration number. Here, it is reported that the chaos signal converges to zero in the Bernoulli shift map with finite resolution [3]. To avoid this zero convergence, the divisor in (3) is modified slightly from 1 to $\lceil 1 - 10^{-16} \rceil$ in the double floating-point calculation. This modification does not affect the randomness of the chaos signal [4]. Furthermore, any chaos equation can be applied in this modulation other than (3) [4, Fig. 8], but (3) is adopted in this study for simplicity.

Then, after iterating (3) $Ite$ times, the processed chaos-modulated symbol $c_{i0}$ is extracted by
\[
\text{Re}[c_{i0}] = x_{i(B+1+\text{mod} N_B)}^{0} + x_{i(2i(B+1)\text{mod} N_B)}^{0}, \quad \text{Im}[c_{i0}] = x_{i(B+1+\text{mod} N_B)}^{0} + x_{i(2i(B+1)\text{mod} N_B)}^{0},
\]

where the iteration number is shifted by another bit of \( b_{i+1} \) from (2). From (2) and (4), random symbols correlated to the transmit bits can be generated. Next, uniformly distributed random signals are generated by the real and imaginary parts of the processed chaos signal \( c_{i0} \) \((1 \leq i \leq N_B)\) as follows:

\[
e_{i0}^{\text{Re}} = \frac{1}{\pi} \arccos(\text{Re}[c_{i0}]), \quad e_{i0}^{\text{Im}} = \frac{1}{\pi} \arcsin(\text{Im}[c_{i0}]) + \frac{1}{2}
\]

In Eq. (5), the two uniform random numbers \( e_{i0}^{\text{Re}} \) and \( e_{i0}^{\text{Im}} \) among \((0, 1)\) are calculated using cosine and sine functions. First, the modulations in (2) are correlated to both real and imaginary components of \( s_{n,j} \) by the summation and subtraction of \( \text{Re}[c_{i0}] \) and \( \text{Im}[c_{i0}] \). Next, two random phases are generated by multiplying different large phase coefficients of \( 37\pi \) and \( 43\pi \). These numbers are arbitrary whenever they are different but double-digit prime numbers are chosen in this study. Then, through the calculation of forward and inverse trigonometric functions, the random numbers \( e_{i0}^{\text{Re}} \) and \( e_{i0}^{\text{Im}} \) are obtained. After that, the Gaussian-distributed transmit symbol is generated by the Box–Muller method as

\[
s_{b_{i0}} = \sqrt{-\log(e_{i0}^{\text{Re}})} \cos(2\pi e_{i0}^{\text{Re}}) + j \sin(2\pi e_{i0}^{\text{Im}}).
\]

The MIMO transmission block \( S_{B,n} \) is composed of \( s_{b_{i0}} \) as follows:

\[
S_{B,n} = \begin{bmatrix}
S_{n,0} & L & S_{n,(B-1)N_r} & M & O & M \\
M & O & M & \cdots & \cdots & \cdots \\
S_{n,N_r-1} & L & S_{n,BN_r-1} & \cdots & \cdots & \cdots \\
S_{n,BN_r} & L & S_{n,(B-1)N_r+1} & \cdots & \cdots & \cdots \\
\end{bmatrix}.
\]

By using the randomization based on Box–Muller method, the Gaussian-distributed signal with a more flat phase characteristic is obtained with a single chaos signal.

### 3 Numerical results

The performance of C-MIMO with the proposed chaos modulation is evaluated by numerical simulations and compared with the performance of conventional C-MIMO [1]. The numbers of transmit and receive antennas are \( N_t = 2 \) and \( N_r = 2 \), respectively. The number of independent chaos sequences in the conventional scheme is ten, and the Gaussian transmission symbols are generated by averaging these ten chaos signals. The C-MIMO block length is \( B = 2, 4, \) and \( 8 \) with the M-algorithm [5]. The channel is assumed as symbol and antenna i.i.d. flat Rayleigh fading, and the receive channel state information is assumed as completely known. The base chaos iteration number \( I_{\text{te}} \) of the conventional and proposed schemes are 19 and 100, respectively, and the adaptive chaos processing scheme with a range of \( M = 2 \) is used to enhance the minimum squared Euclidean distance [1]. The outer channel code is either uncoded or the recursive-systematic convolutional (RSC) code with constraint length 3, code length 2000, and code rate 1/2. S-interleaver is used, and the number of turbo iteration is set to 20.

#### 3.1 Stochastic characteristics of amplitude and phase of transmit signals

The normalized amplitude and phase PDFs of transmit symbol \( s_{b_{i0}} \) are confirmed, as shown in Fig. 2. The results of amplitude distribution (a) are almost
the same for both schemes, while the phase distributions (b) differ between the schemes. In the conventional scheme, the plots fluctuate slightly with lower and higher probabilities in the negative and positive phases, respectively. In contrast, in the proposed scheme, the phase PDF is close to the theoretical value of uniform distribution at $1/2\pi (\approx 0.1592)$. Although it is difficult to make the phase PDF completely uniform at $1/2\pi$ because the transmission bits are correlated to the finite chaos sequence and adaptive chaos processing is adopted, the stochastic characteristics are improved. This implies that the channel coding gain is increased [6].

![Fig. 2. Probability density functions of chaos MIMO transmit symbols: (a) amplitude distribution and (b) phase distribution.](image)

#### 3.2 Bit error rate performance

Fig. 3(a) shows the BER versus average $E_b/N_0$ in the case of uncoded transmission used in the outer channel code. The channel coding effect is obtained in C-MIMO because of the block transmission, compared to that obtained in binary phase shift keying (BPSK)-MIMO-maximum likelihood decoding (MLD), which has the same rate-efficiency as C-MIMO. In addition, it is shown that additional coding gain is obtained in the proposed scheme (labeled as “BM (Box–Muller)” in the figure) compared to the conventional C-MIMO. This is because of the improved randomness of the Gaussian modulation. The gain from the conventional C-MIMO is the best at $B = 4$, and it is
Fig. 3. Bit error rate performances of chaos MIMO; (a) outer uncoded case, (b) concatenation of outer RSC code at rate 1/2 case.

decreases at $B = 8$ with the M-algorithm. It is found that the effect of stochastic characteristic improvement decreases when the M-algorithm is applied. However, the proposed scheme needs only one chaos sequence, which is $1/10^6$ of that required by the conventional C-MIMO; thus, the complexity of signal generation is reduced and the BER is improved.

Next, the BER performance in the case of RSC code concatenation with $B = 4$ is calculated. The results of Fig. 3(b) show that the BER improves in (a) as well. The gains from BPSK-MLSE (joint soft Viterbi decoding for MIMO and RSC code) and conventional C-MIMO are approximately 3 and 0.5 dB, respectively, at $10^{-3}$ of BER. It is shown that the BER improvement is kept in a turbo coding structure.

Consequently, it was shown that the proposed scheme improves the Gaussian signal distribution by the Box–Muller method from one chaos signal, and consequently, the BER performance of C-MIMO was further improved.

4 Conclusions
We proposed a C-MIMO scheme using the Box–Muller method for improving the channel coding effect. In the conventional C-MIMO, a Gaussian transmit signal was composed according to the central limit theorem. However, in the proposed scheme, a more random Gaussian signal was generated from one chaos sequence using the Box–Muller method, which improved the BER performances and reduced the calculation complexities to up to $1/10^\text{th}$ of that obtained through other schemes.

**Acknowledgments**

This research was partially supported by the Scientific Research Grant-in-aid of Japan No. 26420355. The authors wish to express their appreciation for the support received.