Uplink Large-Scale Chaos MIMO Transmission Scheme Using Gaussian Belief Propagation

Naoto Horiike¹, Eiji Okamoto¹, and Tetsuya Yamamoto²

¹ Graduate School of Engineering
Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan
{n.horiike.027, okamoto}@nitech.ac.jp

² Core Element Technology Development Center
Panasonic Corporation, Saedo-cho, Tsuzuki-ku, Yokohama,
Kanagawa 224-8539, Japan
yamamoto.tetsuya001@jp.panasonic.com

Abstract

In this paper, we propose a secure large-scale multiuser multiple-input multiple-output (MU-MIMO) system based on a common-key encryption scheme in uplink. This is a newly proposed large-scale system for a chaos MIMO (C-MIMO) transmission scheme with channel coding and physical layer security effects. However, the calculation complexity for demodulation exponentially increases with the number of transmit antennas in a straightforward conventional large-scale C-MIMO system. Therefore, in this paper, we propose the application of Gaussian belief propagation (GaBP), which is an iterative signal detection method with low calculation complexity, to the C-MIMO scheme. Consequently, we can construct a large-scale MIMO system which has a physical layer security effect with a low calculation complexity, and it is shown that a large channel coding gain can be obtained compared with unencrypted transmission with the same transmission efficiency.

1. Introduction

In future wireless communication systems, the number of wireless terminals is predicted to explosively increase with the progress of technology for the Internet of things (IoT). In such a situation, secure communication systems accommodating a huge number of terminals are strongly needed, for which chaos multiple-input multiple output (C-MIMO) scheme [1] is suitable. Therefore, in this paper, we consider the construction of a large-scale multiuser MIMO (MU-MIMO) system in uplink, that is based on the C-MIMO scheme and has channel coding and physical layer security effects.

On the other hand, large-scale MIMO schemes, in which a base station (BS) has a large number of antennas for simultaneous accommodation of many user equipment (UE), have been extensively studied [2, 3]. The BS with many antennas must separate desired signals from received superposed signals of numerous UEs, and the increasing calculation complexity becomes a problem as the number of users increases. One of the solutions to this problem is Gaussian belief propagation (GaBP), which is a low-complexity iterative signal detection scheme [4, 5]. In large-scale C-MIMO transmission, a similar problem occurs and the calculation complexity at the receiver will exceed the realistic range, because the demodulation is conducted by maximum likelihood sequence estimation (MLSE). Therefore, we propose the application of GaBP to a large-scale C-MIMO system to suppress the calculation complexity. By numerical simulations, we show that the proposed scheme has a channel coding gain compared with a conventional unencrypted scheme with the same transmission efficiency in large-scale MIMO environments as well as a physical layer security effect.

2. Uplink Massive Chaos MIMO Scheme

Figure 1 shows the proposed system model. This system assumes an uplink MU-MIMO environment between K UEs, each with $N_{tu}(1 \leq u \leq K)$ transmitting antennas, and a BS with a $N \times M$ spatial multiplexing transmission from $M$ transmitting antennas in the UE group to $N$ receiving antennas at the BS. In this paper, the relationships of $M = N = N_{tu} \times K$ and $N_{tu} = 1$ are assumed. In addition, the channel is an uncorrelated MIMO channel. In the following, the chaos modulation at each UE and the iterative signal detection with GaBP at the BS are explained.

2.1 Chaos modulation

Chaos modulation is conducted for a transmitting bit sequence consisting of $N_{tu} \times B$ bits at user $u$ as
\[ b_u = \{b_{u,0}, ..., b_{u,N_u-1}\} \quad b_{u,m} \in \{0,1\} \tag{1} \]

where \( B \) is a block length of C-MIMO scheme \([1]\). The following complex symbol sequence is generated as the transmission sequence by the chaos modulation:

\[ x_u = \{s_{u,0}, ..., s_{u,N_u-1}\} \tag{2} \]

where \( 0 \leq m \leq N_uB-1 \). Each UE has a random complex symbol \( c_{0,u} \) as a user-specific initial key signal, where

\[ 0 < \text{Re}[c_{0,u}] < 1, \quad 0 < \text{Im}[c_{0,u}] < 1 \tag{3} \]

The C-MIMO scheme is a common-key encryption scheme and \( c_{0,u} \) is shared between the transmitter and receiver sides. Therefore, in uplink, the BS shares the key with all accommodating UEs for normal common-key encrypted communication. Each UE does not share the key with the BS cannot transmit normally. Each UE conducts the chaos modulation using the key \( c_{0,u} \) and the transmission bit sequence \( b_u \). At the beginning of the modulation process, the convolutional operation using the transmission bit sequence for \( c_{(k-1)} \) in the range of \( 1 \leq k \leq N_uB \) is conducted according to the following rules:

\[ X_0 = \begin{cases} a & (b_{u,m} = 0) \\ 1 - a & (b_{u,m} = 1, a > 1/2) \\ 1 + 1/2 & (b_{u,m} = 1, a \leq 1/2) \end{cases} \tag{4} \]

Real part: \( a = \text{Re}[c_{(k-1)}] \), \( m = k - 1 \)

Imaginary part: \( a = \text{Im}[c_{(k-1)}] \), \( m = k \mod (N_uB) \)

When \( k = 1 \), the initial key itself is used, and the transmission efficiency of this rule is 1 bit/symbol. Then, the variable \( X_0 \) in Eq.(4) is used as the initial signal of chaos generation and is processed by the Bernoulli shift map, which is one of the chaos generation equations, with the iteration number \( l \) given as

\[ X_{l+1} = 2X_l \mod 1 \tag{5} \]

After iterating Eq.(5), the processed chaos-modulated signal \( c_{k,u} \) is extracted by

\[ \text{Real part: } a = \text{Re}[c_{(k-1)}] \] \[ \text{Imaginary part: } a = \text{Im}[c_{(k-1)}] \tag{6} \]

where the subscript of \( X \) indicates the chaos iteration number. In the operation of Eq.(6), the iteration number is shifted by another transmit bit \( b_{u,m} \) and this operation increases the randomness of the generated symbols. Next, the Gaussian distributed symbol \( s_{u,k} \) is modulated by the Box–Muller method \([6]\) as follows:

\[ s_{u,k} = -\ln(c_x^{(k)}) \{\cos(2\pi c_y^{(k)}) \} + j\sin(2\pi c_y^{(k)}) \tag{7} \]

where the uniformly distributed signals \( c_x^{(k)} \) and \( c_y^{(k)} \) are defined as follows:

\[ c_x^{(k)} = \frac{1}{\pi} \cos^{-1}\left[\cos\left(37\pi\text{Re}(c_{k,u}) + \text{Im}(c_{k,u})\right)\right] \]

\[ c_y^{(k)} = \frac{1}{\pi} \sin^{-1}\left[\sin(43\pi\text{Re}(c_{k,u}) - \text{Im}(c_{k,u}))\right] + \frac{1}{2} \tag{8} \]

2.2 Signal detection using GaBP

In the conventional scheme \([1]\), the demodulation of C-MIMO signal at the receiver is conducted by MLSE, and the transmitted sequence is estimated by performing a full-search. Thus, the calculation complexity for the demodulation of one received sequence \( (N_uB \text{ symbols}) \) increases exponentially with the number of transmit antennas and the modulation level, and MLSE is not suitable for a large-scale C-MIMO system with more than about 10 transmit antennas. Therefore, in the proposed scheme, we adopt GaBP, which is an iterative signal detection method with low calculation complexity, for sequence estimation. By using this scheme, parallel interference cancellation (PIC)-based signal detection is possible on a receive antenna basis \([7]\) in a large-scale MIMO system, and the calculation complexity for decoding is reduced compared with that for MLSE. In Fig.1, the signal model at time \( t \) \((0 \leq t \leq B - 1)\) is given by

\[ y(t) = H(t)x(t) + z(t) \tag{9} \]

where \( y(t) \) and \( x(t) \) are the received and transmitted vectors, respectively, and \( z(t) \) is the thermal noise vector. The component of the transmitted vector \( x(t) \) indicates a chaos-modulated symbol in \( x_u \) from a UE at time \( t \). \( H(t) \) is an \( N \times M \) channel matrix at time \( t \), and the \( j \)th row and \( j \)th column element \( h_{j,k} \) is the fading channel coefficient between the \( i \)th \((1 \leq i \leq M)\) transmitting antenna and the \( j \)th \((1 \leq j \leq N)\) receiving antenna. In GaBP, for each receiving antenna, the interference is cancelled by a soft canceller (SC) for each received symbol as follows:

\[ \hat{y}_{j,k} = y_{j,k} - H_{j,k}\hat{x}_{j,k} \tag{10} \]

where \( H_{j,k} \) is the \( j \)th row vector of \( H(t) \) and \( \hat{x}_{j,k} \) is a replica vector consisting of \( M - 1 \) symbols from the transmit antennas excluding the \( i \)th antenna to \( j \)th receiving antenna given by

\[ \hat{x}_{j,k} = [\hat{x}_{j,1}(t), ..., \hat{x}_{j,i-1}(t), 0, \hat{x}_{j,i+1}(t), ..., \hat{x}_{j,M}(t)]^T \tag{11} \]

In this system, each element of Eq.(11) is generated by chaos modulation, and the replica sequence is calculated by Eqs.(4) to (8) with the bit sequence obtained from the hard decision of the prior value \( \lambda_{j,k} \) by the following equation:

\[ \hat{x}_{j,k} = \delta_{s_{u,k}} \tanh \left[ \frac{\lambda_{j,k}}{2} \right] \tag{12} \]

where \( \delta_{s_{u,k}} \) is the chaos-modulated symbol generated from the hard-decided bit sequence and the key signal shared between each UE and the BS, and the replica \( \hat{x}_{j,k} \) is...
calculated by multiplexing \( \hat{s}_{m,k} \) and the reliability information as shown in Eq.(12) [8]. Thus, when the key is unsynchronized between the BS and UEs, the performance of SC deteriorates because different replicas from the transmit symbols are generated. Note that when \( N_{\text{cu}} = 1 \), as assumed in this paper, the ranges of \( k \) and \( t \) are the same, and the \( k \)th symbol of the generated replica sequence is the transmit symbol replica at time \( t \). After the cancellation of interference, the log-likelihood ratio (LLR) is calculated by utilizing \( \hat{y}_{n,m}(t) \). Originally, the LLR was calculated on a symbol basis at each receive antenna in GaBP. However, in chaos modulation, LLR calculation cannot be performed in the antenna or symbol unit because of the convolutional operation with sequence length \( N_{\text{cu}}B \) based on Eq.(4). Therefore, in a large-scale C-MIMO system, the LLR is approximately calculated in the sequence unit by using partial MLSE results from the received sequence \( \hat{y}_{j,t} \) for each UE, which is composed of \( N_{\text{cu}}B \) symbols. First, the demodulation result is obtained by MLSE in terms of \( \hat{y}_{j,t}(t) \) as

\[
\hat{b} = \arg\min_{b_{t/e}} \sum_{t=0}^{B-1} \| \hat{y}_{j,t}(t) - h_j(t)\hat{s}(t) \|^2
\]

(13)

where \( \hat{b} \) is the estimated bit sequence and \( \hat{s}(t) \) is the candidate transmit sequence generated from a bit sequence candidate. Utilizing Eq.(13), the summation of the squared Euclidean distance of the MLSE result is defined as \( d_j^2 \), and the second estimated result \( d_j^2 \) is defined as

\[
d_j^2 = \min_{b_{t/e}} \sum_{t=0}^{B-1} \| \hat{y}_{j,t}(t) - h_j(t)\hat{s}(t) \|^2
\]

(14)

Then, the \( k \)th LLR \( \lambda_j(k) \) in the bit LLR sequence \( \lambda_j \) in the large-scale MIMO system is defined by

\[
\lambda_j(k) = \frac{1}{2\sigma_e^2}(d^2_j - d_k^2)(2\lambda_k - 1),
\]

(15)

where \( \sigma_e^2 \) is the noise variance. In Eq.(15), the value of \( (d^2_j - d_k^2) \) is identical for the entire received sequence at each UE, and only the sign is determined by using the MLSE result \( \hat{b} \). This method is called the sequential LLR method [9,10]. Next, the receive diversity combination is conducted in the probability domain using the LLR sequence \( \lambda_j \) as follows:

\[
\beta_i(k) = \sum_{j=1}^{N} \lambda_j(k)
\]

(16)

where \( \lambda_j \) and \( \beta_i(k) \) are the received bit LLR and the posterior LLR corresponding to the \( k \)th bit in \( N_{\text{cu}}B \) bits transmitted by a certain user, respectively. Here, when \( \beta_i(k) \) in Eq.(16) is simply used as a prior value to generate a replica, the convergence of the iterative operation deteriorates since the correlation between the components of \( \alpha_j(k) \) and the received symbol \( y_j(t) \) is high. Thus, the extrinsic information \( \beta_j(k) \) is constructed and it is fed back as a prior value \( \lambda_j(k) \) as follows:

\[
\lambda_j(k) = \beta_j(k) - \alpha_j(k) = \sum_{j=1}^{N} \alpha_{j,j}(k)
\]

(17)

Here the initial value of \( \lambda_j(k) \) is set to 0. After the iteration based on Eqs.(10), (16), and (17) for a specific number of times, \( \beta_j = \{ \beta_j(0), ... , \beta_j(N_{\text{cu}}B - 1) \} \) at each node is regarded as the LLR sequence \( \beta \) corresponding to the transmitted bits from all users, and the transmitted bit sequences for all users are estimated by the hard decision of \( \beta \).

3. Numerical Simulations

We evaluated the transmission performance of the proposed scheme by numerical simulations with the simulation conditions shown in Table I. In the simulations, an uplink 50 × 50 MIMO environment is assumed, in which 50 UEs are accommodated and each UE has one transmit antenna. The channel is antenna-and-symbol-independent and identically distributed (i.i.d.) and uncorrelated one-pass quasi-static Rayleigh fading, and its channel state information is known to the BS. For a fair comparison, we show the characteristics of a conventional 50 × 50 MU-BPSK-MIMO system as an unencrypted scheme with the same transmission efficiency.

First, we evaluated the convergence of the proposed scheme with the number of iterations in GaBP. Figure 2 shows the average bit error rate (BER) of the system versus the number of iterations of GaBP. Here, the average received \( E_b/N_0 \) is set to 20 dB and the block length \( B \) of the proposed C-MIMO system is set to 2, 3, and 4. In addition, the following equation is used to generate the

| Table I: Basic simulation conditions |
|-------------------------------------|
| Uplink large-scale MU-C-MIMO system |
| No. of users \( K \) | 50 |
| Num. of antennas \( M=N=N_{\text{cu}} \) | \( K = 50, N_{\text{cu}} = 1 \) |
| Chaos modulation | 1 bit/symbol/antenna |
| Chaos generation | Bernoulli shift map |
| No. of chaos processing steps | \( I_{\text{th}} = 100, M = 2 \) [10] |
| Channel | Antenna- and symbol- i.i.d.1 pass quasi-static Rayleigh fading+AWGN |
| Channel state information | Perfect (at the BS) |
| Demodulation | GaBP |
| LLR calculation | Sequential LLR (MLSE) |
tanh

BPSK-MIMO

\[ B \]

C-MIMO, \( B = 3 \)

C-MIMO, \( B = 6 \)

Figure 2: Bit error rate versus iterations of GaBP

\[ \hat{x}_i(k) = \sqrt{E_s} \tanh\left( \frac{\lambda_i(k)}{2} \right) \]  

(18)

where \( E_s \) is the average signal power. It is found that the performance improvement of the C-MIMO system converges in about five iterations when \( B = 2 \), whereas the convergence of the BPSK-MIMO system takes about ten iterations. However, the characteristic of the C-MIMO system with \( B = 2 \) is deteriorated compared with that of the BPSK-MIMO system. In this paper, \( N_{e,m} \) is set to 1, and \( N_{e,m}B \), which is equivalent to the coding length, is 2 when \( B = 2 \). In this case, the improvement effect is quickly finished, because the sequence length of the MLSE is short and the updating effect of LLR accompanying the iteration is reduced. Moreover, because the coding length is too short and the channel coding effect is weak, a sufficient channel coding gain cannot be obtained. Therefore, in the case of \( B = 2 \), BER performance of the proposed scheme is inferior to unencrypted BPSK-MIMO scheme, while the proposed C-MIMO scheme realizes a common-key encryption transmission. On the other hand, by increasing the sequence length to \( B = 3, 4 \), the convergence accompanying the iteration is delayed, although the position of the error floor significantly drops compared with that in BPSK-MIMO transmission. Therefore, when the block length is large, improved BER performance compared with that for the BPSK-MIMO system can be obtained with fewer iterations of GaBP.

Next, we confirmed the performance improvement of the C-MIMO scheme with the block length \( B \) as the parameters when the number of GaBP iterations is fixed to five. Figure 3 shows the average BER versus the average received \( E_b/N_0 \). Here, \( B \) is set to 2, 3, 4, and 6. When \( B = 2 \), characteristic degradation compared with that for the BPSK-MIMO system was confirmed regardless of the average received \( E_b/N_0 \). Whereas, in the case of \( B = 3 \) and above, a large channel coding gain for the unencrypted scheme is obtained in the region where the average received \( E_b/N_0 \) is over 5 dB. This is because of the increase in the channel coding effect with increasing block length. However, increasing \( B \) exponentially increases the calculation complexity for the partial MLSE in Eq.(13). Therefore, it is necessary to appropriately determine the number of iterations and the block length to suppress the amount of calculation. In addition, when unsynchronized users enter the system, the system performance will markedly degrade. By using this characteristic, the intrusion of unauthorized users can be detected and the security of the system is ensured.

4. Conclusions

In this paper, we proposed a large-scale and multiuser chaos MIMO transmission scheme to realize secure and high reliable transmission in an uplink large-scale MIMO environment. To do this, we adopted GaBP, which is an iterative signal detection scheme with low calculation complexity, because the amount of calculations for demodulation by MLSE explosively increases with the number of transmission antennas or users. Consequently, we showed that a channel coding gain could be obtained because of the channel coding effect of chaos modulation, even in a large-scale MIMO system accommodating 50 users.

In future studies, we will consider the improvement of convergence performance by adding damping [5] and evaluate the performance in the case of a larger number of transmitting antennas for each UE.

References

[1] E. Okamoto: A chaos MIMO transmission scheme for channel coding and physical-layer security, IEICE Trans. Commun., Vol. E95-B, No. 4, pp. 1384-1392, 2012.

[2] T. L. Marzetta: Noncooperative cellular wireless with unlimited numbers of base station antennas, IEEE
[3] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors and F. Tufvesson: Scaling up MIMO: Opportunities and challenges with very large arrays, IEEE Signal Process. Mag., Vol. 30, No. 1, pp. 40–60, 2013.

[4] A. Chockalingam: Low-complexity algorithms for large-MIMO detection, Proc. Int’l Symp. on Commun., Control and Signal Processing (ISCCSP), pp.1–6, 2010.

[5] P. Som, T. Datta, A. Chockalingam and B. S. Rajan: Improved large-MIMO detection based on damped belief propagation, Proc. Int’l Telecoms Week (ITW), pp. 1–5, 2010.

[6] G.R.P. Box and M.E. Muller: A note on the generation of random normal deviates, Annals Math. Stat, Vol. 29, pp. 610-611, 1958.

[7] T. Takahashi, S. Ibi, T. Ohgane and S. Sampei: On normalized belief of Gaussian BP in correlated large MIMO channels, Proc. Int’l Sym. on Information Theory and Its Applications (ISITA), pp. 458-462, 2016.

[8] K. Sakoda, H. Hata and S. Hata: Belief-propagation decoding of chaos-modulated signals in massive MIMO systems, IEICE Technical Report, Vol. 117, No. 284, RCS2017-222, pp. 99-103, 2017.

[9] E. Okamoto and Y. Inaba: A chaos MIMO transmission scheme using turbo principle for secure channel-coded transmission, IEICE Trans. Commun., Vol. E98-B, No. 8, pp. 1482-1491, 2015.

[10] E. Okamoto and Y. Inaba: Multilevel modulated chaos MIMO transmission scheme with physical layer security, Nonliner Theory and Its Applications, IEICE, Vol. 5, No. 2, pp. 140-156, 2014.