2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

An EXIT Chart Analysis of Turbo-Coded Chaos MIMO Transmission Scheme

Eiji Okamoto†
†Graduate School of Engineering, Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya 466-8555, Japan.
okamoto@nitech.ac.jp

Abstract– We consider an EXIT chart analysis of turbo-coded chaos multiple-input multiple-output (C-MIMO) scheme. C-MIMO is a transmission scheme having both physical layer security and channel coding gain, and further coding gain can be obtained by applying a turbo principle. Through numerical results of EXIT chart analysis and bit error rate (BER) performance, we show that the output mutual information is continuously increased to (1, 1) point in C-MIMO, and that C-MIMO is suitable for iterative decoding. The consistency of the results between EXIT chart and BER performance is also illustrated.

1. Introduction

Recently, Internet of things (IoT) is becoming widely used, and communication devices associated with human and machines are spatially distributed as a part of social systems. Those devices communicate each other, and the wireless traffic is rapidly growing [1]. On this background, it is important to ensure high-quality and secure transmission in wireless communications. We proposed a chaos multiple-input multiple-output (C-MIMO) scheme to realize this requirement [2]. C-MIMO is a transmission scheme having both physical layer security and channel coding gain, and a turbo-coded transmission is also available by introducing a log-likelihood ratio (LLR), which enables larger coding gain in C-MIMO [3]. Then, it is important to analyze the convergence characteristic of turbo-coded C-MIMO. Here, it is well-known that the convergence characteristics of turbo decoding can be analyzed by EXIT chart [4]. In the EXIT chart, the input-output mutual information of two element decoders is plotted in a same plane in pairs, and the increase of mutual information obtained by iterative decoding can be confirmed on the trajectory of two EXIT curves.

Therefore, in this paper, we analyze the performance of turbo-coded C-MIMO by using EXIT chart. As a result, it is found that the output mutual information is continuously increased in C-MIMO because of rate-1 channel coding property, and that C-MIMO is suitable for iterative decoding. In addition, it is shown that the bit error rate (BER) characteristics of turbo-coded C-MIMO basically coincide the results of EXIT chart analysis.

2. LLR-based chaos MIMO transmission scheme

Figures 1 and 2 show the transmitter and the receiver of C-MIMO transmission scheme, respectively [3]. In the transmitter,

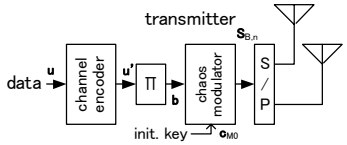

Fig. 1. Code-concatenated chaos MIMO transmitter.

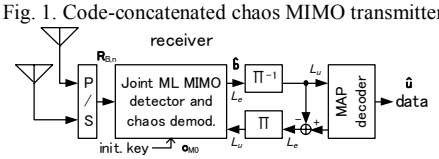

Fig. 2. Turbo-coded chaos MIMO decoder.

data are encoded by the outer channel encoder. After interleaving, the encoded sequence is chaos modulated as the inner encoder and transmitted by the MIMO multiplexing transmission. In the receiver, the joint MIMO detection and chaos demodulation is conducted by MLSE, and the decoder LLR is obtained. After it is deinterleaved, this LLR is handed to the maximum a posteriori probability (MAP) decoder of the outer code. The output LLR is again fed back to the chaos demodulator via the interleaver, and iterative decoding is conducted.

In the transmitter of Fig. 1, a K-bit transmit sequence $\mathbf{u}=\{u_0,\cdots,u_{K-1}\}$, $u_i\in\{0,1\}$ is encoded, and we obtain an N-($>K$) bit sequence $\mathbf{u'}=\{u'_0,\cdots,u'_{N-1}\}$, $u'_i\in\{0,1\}$. Next, $\mathbf{u'}$ is is interleaved to the sequence $\mathbf{b}=\{b_0,\cdots,b_{N-1}\}$. Then, $\mathbf{b}$ is divided per N_tB bit, and is block modulated with block length B by the C-MIMO scheme with a 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 the rate efficiency. Let $\mathbf{b}_n=\{b_{n,0},\cdots,b_{n,N_tB-1}\}=\{b_{nN_tB},\cdots,b_{(n+1)N_tB-1}\}$ as the n-th transmit bit sequence of the n-th C-MIMO block ($0\le n\le(N/N_tB)-1$). $\mathbf{b}_n$ is chaos modulated and the complex symbol sequence $\mathbf{s}_n=\{s_{n,0},\cdots,s_{n,N_tB-1}\}$ is obtained. Then, $\mathbf{s}_n$ is transmitted by the MIMO multiplexing transmission scheme B times for every N_t symbols. The MIMO transmit vector $\mathbf{s}_n(k)$ at time k ($0\le k\le B-1$) is described by

$$\mathbf{s}_n(k)=\{s1(k),\cdots,sN_t(k)\}^T=\{s_{n,kN_t},\cdots,s_{n,(k+1)N_t-1}\}^T,$$

where $si_t(k)$ is the transmit symbol from the i_t-th antenna ($1\le i_t\le N_t$) at time k, and T denotes the transpose. Then, one transmit block is described by

$$\mathbf{S}_{B,n}=\left[\mathbf{s}_n(0),\cdots,\mathbf{s}_n(B-1)\right]$$

The MIMO channel is assumed to be an i.i.d. flat Rayleigh fading channel in terms of the symbol and antenna. When $h_{i_ri_t}(k)$ is the channel component between the i_t-th transmit and i_r-th receive antennas at time k, the channel matrix is given by

$$\mathbf{H}_n(k)=\begin{bmatrix} h_{11}(k) & \cdots & h_{1N_t}(k) \\ \vdots & \ddots & \vdots \\ h_{N_r1}(k) & \cdots & h_{N_rN_t}(k) \end{bmatrix},$$

where N_r is the number of receive antennas. Then, the receive MIMO vector $\mathbf{r}_n(k)=\{r1(k),\cdots,rN_r(k)\}^T$ at time k becomes

$$\mathbf{r}_n(k)=\mathbf{H}_n(k)\mathbf{s}_n(k)+\mathbf{n}_n(k),$$

where $\mathbf{n}_n(k)=\{n1(k),\cdots,nN_r(k)\}^T$ is a zero-mean Gaussian noise vector with the same variance. The receive block then becomes

$$\mathbf{R}_{B,n}=\left[\mathbf{r}_n(0),\cdots,\mathbf{r}_n(B-1)\right]$$

2. 1 Framework of chaos modulation

The framework of 1-bit/symbol/antenna chaos modulation generating $\mathbf{S}_{B,n}$ from $\mathbf{b}_n$ is described in [3], and to enhance the channel coding gain, the adaptive chaos iteration scheme [5] is applied. The details are omitted here due to space limitation.

2. 2 Iterative decoding using sequential LLR

We perform the joint MIMO detection and chaos demodulation in the demodulator of the receiver. Because the chaos modulation is a non-systematic nonlinear modulation and the signal constellation is not fixed, bit LLR cannot be calculated in the usual manner. Therefore, we calculate a single likelihood ratio for every C-MIMO transmission block, and the absolute value of the likelihood ratio is used as bit LLRs in that block. In addition, taking advantage of the fact that the chaos modulation structure is the same as that of the multipath channel, the extrinsic LLR is calculated in the same manner as the minimum mean square error (MMSE) filter of turbo equalization [6]. The assumption is made that the squared Euclidean distance between the received and estimated sequences outputted at the chaos demodulator is a Gaussian distribution.

In the receiver of Fig. 2, the demodulated bit LLR of C-MIMO is calculated for the receive block, $\mathbf{R}_{B,n}$. First, the demodulation result is obtained by MLSE as

$$\begin{aligned}\hat{\mathbf{b}}_n &= \{\hat{b}_{n,0},\cdots,\hat{b}_{n,N_tB-1}\} \\ &= \arg\min_{\mathbf{b}_n,Ite}\sum_{k=0}^{B-1}\frac{1}{2\sigma_e^2}\left\|\mathbf{r}_n(k)-\mathbf{H}_n(k)\mathbf{s}_n(k)\right\|^2-\sum_{i=0}^{N_tB-1}\frac{1}{2}L_u(\hat{b}_{n,i})\end{aligned}, \quad (1)$$

where $L_u(\hat{b}_{n,i})$ ($0\le n\le (N/N_tB)-1$, $0\le i\le N_tB-1$) is the a priori LLR handed by the latter MAP decoder, and is zero at the first iteration, σ_e^2 is the noise variance, and *Ite* is the chaos iteration number [3]. The right hand side of (1) can be used as the metric of maximum likelihood detection in MIMO [7 (19), 8]. Then, the metrics of (1) for $\hat{b}_{n,i}=0$ and 1 at time *i* are calculated and the extrinsic bit LLR of $\hat{b}_{n,i}$ is obtained by the difference between them as follows [7 (5), 8 (18)].

$$\begin{aligned}L_e\left(\hat{b}_{n,i}\right)_{Ite} &= \min_{\hat{b}_{n,i}=0}\left[\sum_{k=0}^{B-1}\frac{1}{2\sigma_e^2}\left\|\mathbf{r}_n(k)-\mathbf{H}_n(k)\mathbf{s}_n(k)\right\|^2\Big|_{Ite}-\sum_{j=0}^{N_tB-1}\frac{1}{2}L_u(\hat{b}_{n,j})\right] \\ &\quad -\min_{\hat{b}_{n,i}=1}\left[\sum_{k=0}^{B-1}\frac{1}{2\sigma_e^2}\left\|\mathbf{r}_n(k)-\mathbf{H}_n(k)\mathbf{s}_n(k)\right\|^2\Big|_{Ite}-\sum_{j=0}^{N_tB-1}\frac{1}{2}L_u(\hat{b}_{n,j})\right]\end{aligned} \quad (2)$$

In the calculation of (2), the symbol-by-symbol MAP algorithm can be applied for each *i* when the modulation is linear, and then, the number of sequence search in (2) becomes 2^{N_tB} for $\hat{\mathbf{b}}_n$. However, because C-MIMO is a nonlinear nonsystematic convolutional modulation, the modulated signal at time *i* changes also according to bit sequence other than *i*. Then, the number of sequence search to calculate LLRs of $\hat{\mathbf{b}}_n$ becomes $N_tB\cdot 2^{N_tB}$, which is highly complex. Therefore, to reduce the complexity to calculate the LLR in C-MIMO, we assume that the *sequence* likelihood of MLSE result is almost the same as each *bit* likelihood of MLSE result. Then, the bit LLRs are derived with 2^{N_tB} searches. The summation of the squared Euclidean distance of the MLSE result is defined by

$$d_1^2=\sum_{k=0}^{B-1}\frac{1}{2\sigma_e^2}\left\|\mathbf{r}_n(k)-\mathbf{H}_n(k)\mathbf{s}_n(k)\right\|^2\Big|_{Ite}-\sum_{i=0}^{N_tB-1}\frac{1}{2}L_u(\hat{b}_{n,i})\Big|_{\hat{\mathbf{b}}_n} \quad (3)$$

and the second best result is defined as

$$d_2^2=\min_{\mathbf{b}_n\neq\hat{\mathbf{b}}_n}\left[\sum_{k=0}^{B-1}\frac{1}{2\sigma_e^2}\left\|\mathbf{r}_n(k)-\mathbf{H}_n(k)\mathbf{s}_n(k)\right\|^2\Big|_{Ite}-\sum_{i=0}^{N_tB-1}\frac{1}{2}L_u(\hat{b}_{n,i})\right] \quad (4)$$

Then, the extrinsic LLR of the C-MIMO demodulator is derived by

$$L_e\left(\hat{b}_{n,i}\right)_{Ite}=\left(d_2^2-d_1^2\right)\left(2\hat{b}_{n,i}-1\right),\quad 0\le i\le N_tB-1, \quad (5)$$

where the absolute value is the same as in the block and the sign corresponds to each bit. Because the bit LLR of (5) is derived by the difference between the best and the second best demodulated results of sequences (3) and (4), hereafter, we refer to it as the sequential LLR. Furthermore, it is assumed that the sequential LLR is not correlated to the a priori bit LLR $L_u(\hat{b}_{n,i})$ because the modulated signal is a non-systematic random Gaussian. Then, the LLR in (5) is used not as a posteriori LLR but as an extrinsic LLR [6]. After the extrinsic LLRs of all blocks are calculated and deinterleaved, we obtain the a priori LLR $L_u(\hat{x}_i)$ ($0\le i\le N-1$) for the MAP decoder. In the MAP decoder, the posteriori LLR is calculated using the Bahl, Cocke, Jelinek, and Raviv (BCJR) algorithm and the extrinsic LLR $L_e(\hat{x}_i)$ is obtained. Then, after interleaving, the a priori $L_u(\hat{b}_{n,i})$ is again inputted to the C-MIMO demodulator, and Eqs. (1) to (4) are iterated. This turbo iteration is repeated and the decoded bit $\hat{\mathbf{u}}=\{\hat{u}_0,\cdots,\hat{u}_{K-1}\}$ is determined by the posteriori LLR of the MAP decoder.

3. EXIT chart analysis

EXIT chart analysis [4] is a visualization scheme of convergence characteristics on turbo codes. In the EXIT chart, the input-output mutual information of two element decoders is plotted in a same plane in pairs, and the increase of mutual information obtained by iterative decoding can be confirmed by the trajectory of two EXIT curves. The mutual information is calculated by LLR of transmitted bits and has the value between 0 and 1. Here, we assume that the extrinsic LLR $L_e\left(\hat{b}_{n,i}\right)$ of C-MIMO decoder and the extrinsic LLR $L_e(\hat{x}_i)$ of outer channel decoder satisfy *the consistency condition* as follows.

$$L_e\left(\hat{b}_{n,i}\right)=\mu\left(2b_{n,i}-1\right)+v$$
$$L_e(\hat{x}_i)=\mu(2x_i-1)+v$$

Here, v is a Gaussian noise element with $v\in N(0,\sigma_v^2)$ and $\mu=\sigma_v^2/2$. Then, the standard deviation σ_v and the mutual information I_a can be calculated each other by J-function and its approximate expression as follows.

$$\sigma_v=J^{-1}(I_a)\approx\left\{-\frac{1}{H_1}\log_2\left(1-I_a^{\frac{1}{H_3}}\right)\right\}^{\frac{1}{2H_2}} \quad (6)$$

$$I_a=\frac{1}{2}\sum_{x=0,1}\int_{-\infty}^{\infty}p_e(\xi\mid X=x)\log_2\frac{2p_e(\xi\mid X=x)}{\sum_{x'=0,1}p_e(\xi\mid X=x')}d\xi \quad (7)$$

Here, $H_1=0.3073$, $H_2=0.8935$, $H_3=1.1064$, and $p_e(\xi\mid X=x)$ is the conditional probability density function of extrinsic LLR when the received bit is $x=0,1$. Hence, the standard deviation σ_v is obtained for one mutual information I_{a_CMIMO} by (6) and a prior LLR $L_u(\hat{b}_{n,i})$ is calculated using σ_v. These $L_u(\hat{b}_{n,i})$ is then entered into C-MIMO decoder with received symbols and the extrinsic LLR $L_e(\hat{b}_{n,i})$ is obtained. Calculating the probability density function of this $L_e(\hat{b}_{n,i})$ the mutual information I_{e_CMIMO} is obtained by (7). In the same way, for the outer channel decoder, using one mutual information I_{a_CC} (channel coding: CC), the standard deviation σ_v is

Table 1 Simulation conditions.

		C-MIMO
Modulation		Chaos-based Gaussian, 1 bit/symbol
Num. of antennas		$N_t = N_r = 2$
MIMO block length		$B = 2, 4, B = 8$ with M-arighrithm
Chaos		Bernoulli shift map
Num. of chaos processing		$Ite = 19$, $M = 2$
Initial chaos synchronization		Perfect
Channel		Symbol-i.i.d. 1-path Rayleigh fading
Receive channel state inf. (CSIR)		Perfect
MIMO detection & decode		Soft-MLSE + BCJR
Outer channel code		Recursive-systematic convolutional (RSC) code, rate 1/2, N=2000, constraint 3
		Low-density parity check (LDPC) code, rate 0.902, N=930, K=839
BER simulation	Interleaver	S-random
	Max. num. of turbo iteration	20

obtained. A prior LLR $L_u(\hat{x}_i)$ is calculated and handed to the channel decoder. Using the output of the decoder, the extrinsic LLR $L_e(\hat{x}_i)$ is calculated, and I_{e_CC} is obtained by the probability density function of $L_e(\hat{x}_i)$ and (7).

The EXIT chart is drawn by the curves of $I_{a\_CMIMO} - I_{e\_CMIMO}$ and $I_{a\_CC} - I_{e\_CC}$, in which the axes of I_{a_CMIMO} and I_{e_CC} are overlapped as well as the axes of I_{e_CMIMO} and I_{a_CC}. When there is no intersection between two curves, the mutual information converges at (1, 1) point, which means the correct transmission bits $\hat{\mathbf{u}}$ are obtained by the iterative decoding between C-MIMO decoder and outer channel decoder. If the intersection exists, better bit error rate is obtained when the coordinate of intersection is at right-upper region, close to (1,1).

4. Numerical results

The performance of C-MIMO scheme is evaluated by computer simulations using the parameters in Table 1. The outer code is the convolutional code and low-density parity check (LDPC) code. The number of MIMO antennas is $N_t = N_r = 2$, and the C-MIMO block length is B = 2 to 8. The base iteration number of chaos is set to I_0 = 19, and is determined by performing a numerical search, but this number does not affect the BER performance, and the adaptive chaos processing scheme with M = 2 is used [5]. The maximum number of turbo iterations is 20.

Fig. 3 shows the input-output characteristics of mutual information in C-MIMO without outer channel codes. It is shown that the output mutual information I_e is increasing for the input mutual information I_a in all schemes. Compared with BPSK-MIMO-MLD scheme, the output I_e is rapidly increasing with higher input I_a in C-MIMO because of the channel coding property, and I_e reaches (1, 1) point. Furthermore, when B = 8 with applying M-algorithm (its complexity is equivalent to B = 5) [9], the higher I_e is obtained in whole. Thus, it is expected in C-MIMO that a larger coding gain is obtained when an outer channel code is concatenated and the iterative decoding is conducted.

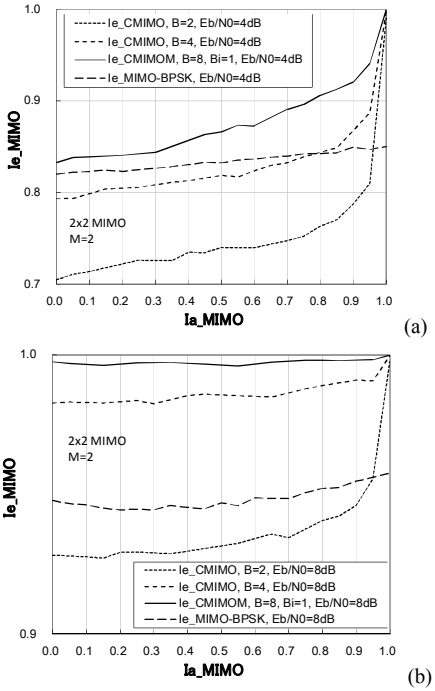

Fig. 3. Input-output characteristics of mutual information in C-MIMO without outer channel codes; (a) E_b/N_0 = 4 dB, (b) E_b/N_0 = 8 dB.

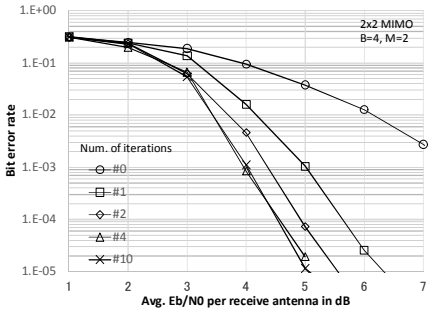

Fig. 4. BER performance of C-MIMO for various number of turbo iterations.

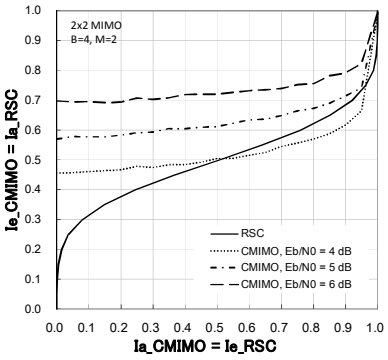

Fig. 5. EXIT chart of C-MIMO with convolutional code.

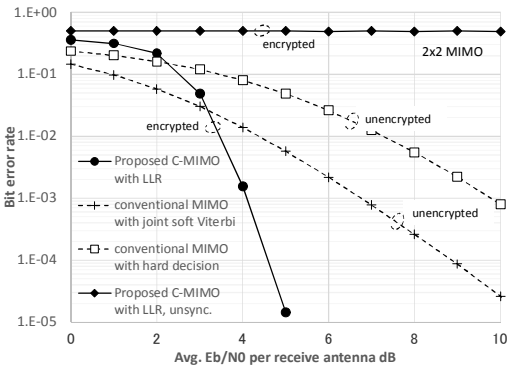

Fig. 6. Comparison of BER performance versus average E_b/N_0 when outer convolutional code is concatenated.

Next, the BER versus the average E_b/N_0 with the parameter of he maximum turbo iteration number is calculated. Hereafter, the block length of $B = 4$ is used. The result in Fig. 4 shows that the turbo principle works in C-MIMO scheme, and the BER is improved according to the iteration number. In particular, the first iteration significantly improves the performance as a normal turbo decoding. However, the BER then converges because the block length of C-MIMO is short, and it becomes almost fixed at 10 iterations. Fig. 5 shows the EXIT chart of this scheme and the result supports the BER improvement in Fig. 4. In the first iteration, the great increase of mutual information is obtained, and after $E_b/N_0 = 5$ dB, the mutual information of 1 is obtained after iteration.

Then, the BER performance with a maximum iteration number of 20 is compared to that of conventional schemes at the same rate efficiency. The hard Viterbi decoding concatenated from MIMO-MLD and the soft decoding using a joint trellis diagram for MIMO detection and an outer convolutional code are considered as the conventional schemes. The transmission efficiency for all schemes is 1/2 bit/symbol. Fig. 6 shows the results obtained. In the conventional scheme, the joint soft Viterbi decoding of the MIMO and convolutional code becomes MLSE and optimal. In C-MIMO, we show that the BER is degraded at the low E_b/N_0 region, and is rapidly improved because of the turbo principle. After $E_b / N_0 \geq 4$ dB, which is different from the normal turbo equalization, the BER does not converge to MIMO-MLSE or improve because of the channel coding effect of C-MIMO. In addition, because C-MIMO has the property of encryption, we realized a LLR-based channel decoding scheme with physical layer security. In Fig. 6, the BER of C-MIMO at the eavesdropper that has a difference of 10^{-3} Euclidean distances in the initial key symbol is almost 0.5, which indicates that the common key-based secure communication has been realized. It is

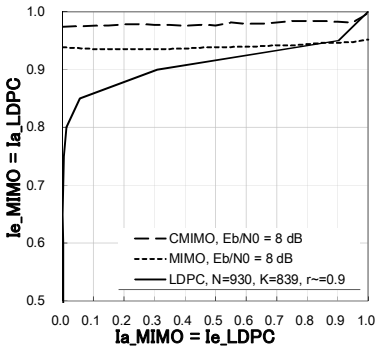

Fig. 7. EXIT chart comparison of proposed C-MIMO and MIMO with outer LDPC codes at Eb/N0 = 8 dB.

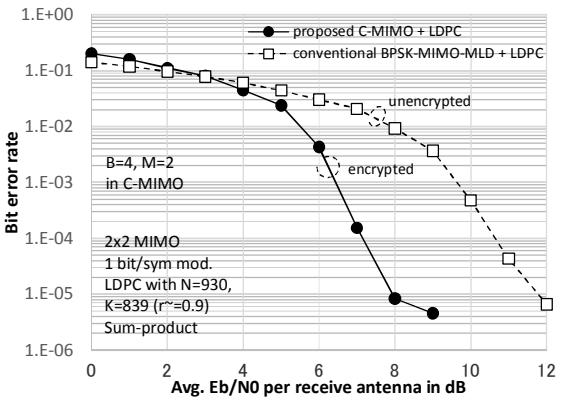

Fig. 8. BER performance versus average E_b/N_0 when outer LDPC codes are concatenated at rate 0.9.

described in [10] that the secrecy capacity is equivalently calculated by the bit error rate.

The case of LDPC concatenation is also considered. The configuration of outer LDPC codes are listed in Table 1, and the results are shown in Figs. 7 and 8. In Fig. 7, the EXIT chart at $E_b/N_0 = 8$ dB is plotted, where the raw BER performance of C-MIMO will be slightly better than that of MIMO. The result of Fig. 7 shows that the better BER is expected after decoding iteration in C-MIMO because the eye pattern between the inner (C-)MIMO and the outer LDPC code is wider in C-MIMO. From Fig. 8, it is shown that the BER performances reflect the EXIT chart analyses.

5. Conclusions

We considered an EXIT chart analysis of turbo-coded C-MIMO introducing LLR and iterative soft-valued decoding, and compared its results with the BER performances through numerical simulations. As a result, it is shown that the mutual information of C-MIMO reaches (1, 1) point, that means the turbo-coded C-MIMO will have better BER performance with an out channel code concatenation on proper configurations.

In future studies, a turbo code design of C-MIMO having better performance at lower E_b/N_0 region will be considered using EXIT chart analysis.

Acknowledgments

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

References

[1] ARIB 2020 and Beyond Ad Hoc Group, “Mobile Communications Systems for 2020 and beyond,” White Paper, [Online] http://www.arib.or.jp/ADWICS/20bah-wp-100.pdf, Oct. 2014.

[2] 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, Apr. 2012.

[3] 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, Aug. 2015.

[4] S. ten Brink, “Convergence behavior of iteratively decoded parallel concatenated codes,” IEEE Trans. on Commun., vol. 49, no. 10, pp. 1727-1737, Oct. 2001.

[5] E. Okamoto and Y. Inaba, “Multilevel Modulated Chaos MIMO Transmission Scheme with Physical Layer Security,” Nonlinear Theory and Its Applications, IEICE, vol. E5-N, no. 2, Apr. 2014.

[6] M. Tüchler, R. Koetter, and AC. Singer, "Turbo equalization: principles and new results," IEEE Trans. on Commun., vol. 50, no. 5, pp. 754-767, May 2002.

[7] B. Steingrimsson, Z.-Q. Luo, K. M. Wong, "Soft quasi-maximum-likelihood detection for multiple-antenna wireless channels," IEEE Trans. Signal Processing, vol.51, no.11, pp. 2710-2719, Nov 2003.

[8] S. Baro, J. Hagenauer, M. Witzke, "Iterative detection of MIMO transmission using a list-sequential (LISS) detector," IEEE Int'l Conf. Communications (ICC2003), vol.4, no., pp. 2653-2657, May 2003.

[9] E. Okamoto and Y. Inaba, “Study on decoding complexity reduction of chaos MIMO transmission scheme by applying M-algorithm,” IEICE Tech. Rep., vol. 114, no. 254, RCS2014-181, pp. 141-146, Oct. 2014. (in Japanese)

[10] M. Baldi, M. Bianchi, F. Chiaraluce, ``Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 883-894, Jun. 2012.