

## Paper

# Multi-user chaos MIMO-OFDM scheme for physical layer multi-access security

*Yuma Inaba<sup>1a)</sup> and Eiji okamoto<sup>1b)</sup>*

<sup>1</sup> *Department of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology  
Gokiso-cho, Showa-ku, Nagoya-shi, Aichi-ken 466-8555, Japan*

<sup>a)</sup> *cju17512@stn.nitech.ac.jp*

<sup>b)</sup> *okamoto@nitech.ac.jp*

Received July 12, 2013; Revised November 16, 2013; Published April 1, 2014

**Abstract:** Wireless multihop networks can be potentially used to realize a smart community that comprehensively controls social infrastructures. In a wireless multihop transmission, personal data are forwarded by a third party, so wireless security is indispensable. In current wireless systems, security is ensured by encryption in the upper layers. However, this encryption tends to require a complex protocol or processing, which is not suitable for a multihop protocol with a simple implementation. To solve this problem, we have proposed a chaos multiple-input multiple-output orthogonal frequency division multiplexing (MIMO-OFDM) scheme with physical layer encryption and channel-coding abilities. On the other hand, an effective technique for wireless multihop transmission is point-to-multipoint (P-MP) communication, and recently, multi-user (MU)-MIMO has been proposed as an effective P-MP scheme. In MU-MIMO, wireless security is also important. However, there are few studies considering MU-MIMO security in the physical layer. Therefore, in this paper, we propose a multiuser (MU) chaos MIMO-OFDM scheme that achieves physical layer security and channel-coding gain in MU-MIMO transmission. Additionally, the user distribution and propagation loss are taken into consideration. The improved performances are shown through computer simulations.

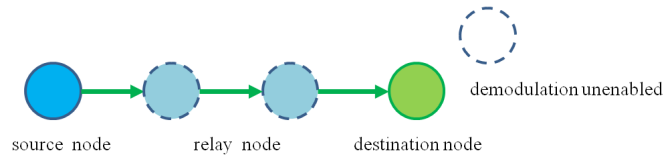
**Key Words:** multihop communications, encryption, chaos, MU-MIMO

## 1. Introduction

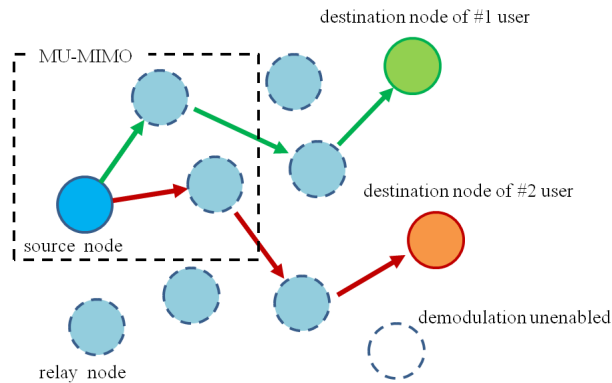
In wireless communications, frequency bands are a limited resource, and improvement in spectral efficiency is always desired. Additionally, it is not practical to expand a frequency band for one user for higher-capacity transmissions. A multiple-input multiple-output (MIMO) technique in which multiple antennas in both the transmitter and receiver simultaneously communicate using the same frequency band can increase the channel capacity without expanding the frequency band and is drawing significant attention. The transmission rate can be increased in proportion to the minimum numbers of transmit and receive antennas. However, in mobile terminals such as smart phones, the number of antennas and the signal processing ability are limited by the restriction of the package and battery sizes, and the capacity enhancement of MIMO is restricted by the mobile terminal limitation

even if the base station can prepare many antennas. To address this problem, multiuser MIMO (MU-MIMO), a type of advanced MIMO technique, has been proposed in which spatial multiple access can be achieved and in which the system capacity is increased even with a single antenna of a mobile terminal. As a result, many improved MU-MIMO systems have been studied [1–4]. In MU-MIMO, beamforming is conducted at the transmitter to avoid signals for multiple receivers interfering with each other. In particular, the transmitter adjusts the transmit weights multiplied by each transmit symbol of the MIMO system according to the channel matrix between the transmitter and all receivers so as to make the signal of each user orthogonal. By this orthogonal beamforming, interference-free simultaneous transmission is achieved.

On the other hand, along with the development of wireless technologies, a smart community system has been developed with the use of wireless multihop transmission, e.g., smart meters. In those wireless multihop transmissions, personal data are transmitted via the terminal of a third party, thus ensuring that security is indispensable. In multihop transmissions, as shown in Fig. 1, data are forwarded by relay nodes using a forwarding protocol such as amplify and forward (AF), decode and forward (DF), or detect and forward (DetF) [5]. It is desirable that relay nodes cannot decode the forwarding data. Usually the encryption is conducted with the upper layer protocols. However, complicated processes with increased complexity are needed when a complicated secure protocol is used in the implementation. To solve this problem, we have proposed a MIMO multiplexing transmission with a physical layer security technique called chaos MIMO (C-MIMO) in [6, 7]. This technique works by ensuring that, with the physical layer security, the upper layer secure protocols can be omitted and that the increase in complexity can be restricted. In C-MIMO, the modulated signals are generated by utilizing the deterministic and irregular characteristics of chaos, introduced by the principle of chaos communication. In addition, rate-one channel coding is conducted by using chaos signals correlated with transmit bits. Hence, the physical-layer security and channel coding gain are obtained in a trade-off with the increase in the decoding search. As stated above, security also has to be ensured in multihop transmission and wireless multiple access networks, and MU-MIMO realizing one-to-many communications with the physical layer security is effective in terms of a multiple-access scheme, spectral efficiency, and a secure protocol. In [8], the application of C-MIMO into AF multihop transmission has been proposed, and the effectiveness of security and cooperative diversity has been demonstrated. In a multihop transmission, as in Fig. 1, when only the source and the destination nodes have a shared secret key, the relay nodes cannot decode the forwarding data, but the destination can decode the forwarded data and can also take advantage of cooperative diversity. Furthermore, as shown in Fig. 2, if C-MIMO and MU-MIMO are combined, secure multiuser multihop transmission



**Fig. 1.** Multihop transmission.



**Fig. 2.** MU-Multihop transmission.

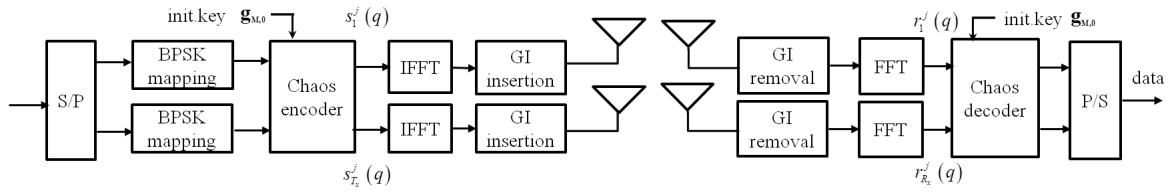
is expected to be successful.

However, the application of C-MIMO into MU-MIMO has not been considered yet. Therefore, in this paper, to achieve a secure multiuser multihop transmission, we propose a multiuser chaos MIMO-orthogonal frequency division multiplexing (OFDM) scheme enabling multiuser transmission and considering propagation loss with physical layer security and channel coding gain by applying C-MIMO to MU-MIMO. Additionally, the user distribution and the propagation loss are taken into consideration. Here, to focus on the secure MU-MIMO architecture, it is assumed in this paper that the receive users of MU-MIMO in Fig. 2 are not the relay nodes but the destination users for simplicity.

In the following, the chaos MIMO-OFDM transmission scheme and the proposed MU-C-MIMO-OFDM scheme are introduced in Sections 2 and 3. The numerical results in which security is ensured and the coding gain is improved according to the number of users are shown in Section 4, and conclusions are drawn in Section 5.

## 2. Chaos MIMO-OFDM system

Figure 3 shows the baseband system model of C-MIMO-OFDM [6], where  $T_x$  and  $R_x$  are the numbers of transmit and receive antennas, respectively. The chaos encoder and decoder are inserted into the conventional MIMO-OFDM system. The variables in the figure are introduced in the following subsections.



**Fig. 3.** System block diagram of chaos MIMO-OFDM.

### 2.1 Transmit and receive symbols

In C-MIMO-OFDM, the transmit data in one OFDM frame is denoted by a complex vector as

$$\mathbf{d} = (d_0, \dots, d_{T_x N - 1}) \quad (1)$$

where  $N$  is the number of subcarriers. The block transmission is adopted to obtain the channel coding gain. When  $B$  is defined as the chaos block length, the  $j$ -th data block is given from (1) as

$$\mathbf{d}^j = (d_0^j, \dots, d_t^j, \dots, d_{T_x B - 1}^j) \quad (2)$$

where  $0 \leq j \leq N/B - 1$ . Then, the complex chaos vector corresponding to the data block is prepared as

$$\mathbf{c} = (c_0, \dots, c_t, \dots, c_{T_x B - 1}) \quad (3)$$

and the multiplied vector at each element

$$\begin{aligned} \mathbf{s}^j &= \mathbf{c} * \mathbf{d}^j = (c_0 d_0^j, \dots, c_t d_t^j, \dots, c_{T_x B - 1} d_{T_x B - 1}^j) \\ &= (s_0^j, \dots, s_t^j, \dots, s_{T_x B - 1}^j) \end{aligned} \quad (4)$$

is the transmit symbol at the  $j$ -th block, where each element is allocated to a different subcarrier of OFDM, and the generation method of  $\mathbf{c}$  is described in Subsection 2.3. The transmit sequence of the  $j$ -th block from the  $l$ -th MIMO transmit antenna is defined as

$$\begin{aligned} \mathbf{s}_l^j &= (s_{B(l-1)}^j, \dots, s_{B l - 1}^j) \\ &= (s_l^j(0), \dots, s_l^j(q), \dots, s_l^j(B - 1)) \end{aligned} \quad (5)$$

where  $1 \leq l \leq T_x$ . Then, the  $l$ -th antenna transmits the sequence of

$$\mathbf{s}_l = (\mathbf{s}_l^0, \dots, \mathbf{s}_l^j, \dots, \mathbf{s}_l^{N/B-1}) \quad (6)$$

Similarly to (5), the receive sequence is defined by

$$\mathbf{r}_m^j = (\mathbf{r}_m^j(0), \dots, \mathbf{r}_m^j(q), \dots, \mathbf{r}_m^j(B-1)) \quad (7)$$

where  $m$  is the number of receive antennas, and  $1 \leq m \leq R_x$ .

## 2.2 Maximum likelihood sequence estimation in decoder

Let us consider the transmit and receive vectors of the  $q$ -th symbol  $0 \leq q \leq B-1$  in the  $j$ -th block as

$$\begin{aligned} \mathbf{s}^{j,q} &= [s_1^j(q), \dots, s_{T_x}^j(q)]^T \\ \mathbf{r}^{j,q} &= [r_1^j(q), \dots, r_{R_x}^j(q)]^T \end{aligned}$$

where  $T$  is the matrix transpose. When the channel matrix between the transmitter and the receiver at the  $q$ -th symbol (subcarrier) at the  $j$ -th block is given by

$$\mathbf{H}^{j,q} = \begin{bmatrix} H_{11}^j & \cdots & H_{1T_x}^j \\ \vdots & \ddots & \vdots \\ H_{R_x1}^j & \cdots & H_{R_xT_x}^j \end{bmatrix} \quad (8)$$

Then, the decoded sequence  $\hat{\mathbf{s}}^j$  at the  $j$ -th block can be obtained by the maximum likelihood sequence estimation (MLSE) as

$$\hat{\mathbf{s}}^j = \arg \min_{\mathbf{s}^j} \sum_{q=0}^{B-1} \|\mathbf{r}^{j,q} - \mathbf{H}^{j,q} \mathbf{s}^{j,q}\| \quad (9)$$

Thus, the joint block decoding in terms of the chaos decoding and MIMO detection is conducted.

## 2.3 Generation of chaos symbols

The generation method of the chaos symbols in (3) is described below. To obtain the channel coding gain, the chaos symbols generated are correlated to the data vector of (2). The  $t$ -th chaos symbol of (3) is generated by

$$c_t = \exp(j2\pi \arctan(\Im[s_t]/\Re[s_t]))$$

Here,  $0 \leq t \leq T_x B - 1$ , and  $s_t$  is a pseudorandom Gaussian symbol given by

$$s_t = \frac{1}{M} \sum_{i=0}^{M-1} (\Re[g_{ti}] + \Im[g_{ti}]) \exp(j8\pi[\Re[g_{gi}] - \Im[g_{ti}]])$$

where  $g_{ti}$  is the  $i$ -th of  $M$  chaos element symbols at index  $t$ .  $M$  is the number of chaos element symbols to make  $s_t$  Gaussian symbols by the central limit theorem. Because  $c_t$  is a unit vector with a random phase, the encryption of  $\mathbf{d}^j$  in (4) is executed by the phase shift operation, and the signal power of  $\mathbf{s}^j$  is not changed by  $\mathbf{c}$ . Here, let  $M$  chaos element symbols be denoted as

$$\mathbf{g}_{M,t} = (g_{t0}, \dots, g_{t(M-1)}), 0 < \Re[g_{ti}], \Im[g_{ti}] < 1 \quad (10)$$

and its initial vector is denoted by

$$\mathbf{g}_{M,0} = (g_{00}, \dots, g_{0(M-1)})$$

This  $\mathbf{g}_{M,0}$  becomes the key vector shared by the transmitter and the receiver. Thus, the proposed C-MIMO scheme is a type of common key encryption. The chaos element symbols of (10) are iteratively calculated by the following equations of (11)–(14).

$$x_0 = \begin{cases} \Re[g_{(t-1)i}] & (b_m = 0) \\ 1 - \Re[g_{(t-1)i}] & (b_m = 1, \Re[g_{(t-1)i}] > 1/2) \\ \Re[g_{(t-1)i}] + 1/2 & (b_m = 1, \Re[g_{(t-1)i}] \leq 1/2) \end{cases} \quad (11)$$

$$y_0 = \Im[g_{(t-1)i}] \quad (12)$$

$$x_{l+1} = 2x_l \bmod 1, \quad y_{l+1} = 2y_l \bmod 1 \quad (13)$$

$$\Re[g_{ti}] = x_{BO+b_m}, \quad \Im[g_{ti}] = y_{BO+b_m} \quad (14)$$

Here,  $BO$  is a positive constant,  $m = (t + T_x B - 1) \bmod T_x B$ , and  $b_m$  is the transmit bit corresponding to the  $m$ -th data symbol  $d_m^j$  in the  $j$ -th block. Thus, the chaos symbols are correlated with the transmit bits in the same block, and the convolutional channel coding effect is obtained. Equation (13) is the Bernoulli shift map and makes  $g_{ti}$  chaotic.

## 2.4 Bit error rate performance of C-MIMO-OFDM

Here, the performance of the C-MIMO-OFDM scheme is evaluated through computer simulations with the parameters of Table I. It is assumed that the channel is an antenna-i.i.d. and OFDM frame-i.i.d. 1-dB decaying 9-path quasi-static Rayleigh fading channel and that the receiver perfectly knows the channel. The chaos maps are the Bernoulli shift map of (13) and the Tent map given by

$$a_{l+1} = \begin{cases} 2a_l & (a_l < 0.5) \\ 2a_l(1 - a_l) & (0.5 \leq a_l) \end{cases}$$

The chaos initial value  $\mathbf{g}_{M,0}$  is randomly changed on every chaos block to obtain the average performance. Figure 4 shows the bit error rate (BER) after the MLSE decoding of (9). It is shown that the performance of C-MIMO-OFDM is superior to that of unsecured MIMO transmission with MLD. This improvement is achieved by the convolutional coding effect of chaos. In addition, it is confirmed that the BER is not affected by the use of different maps because the chaos encoding is conducted by the random phase shift in C-MIMO, as described in (4) and Subsection 2.3. Therefore, the Bernoulli shift map whose generation and implementation are simple is used in this paper.

**Table I.** Simulation conditions of C-MIMO-OFDM.

Modulation	BPSK		
Num. of 1OFDM symbols	64		
Num. of transmit antenna $T_x$	2		
Num. of receive antenna $R_x$	2		
Chaos	N/A	Bernoulli shift map	tent map
Num. of MIMO symbols on 1 block $B$	N/A	4	
Num. of chaos signals $M$	N/A	10	
Num. of chaos iteration $BO$	N/A	19	
Channel	1-dB decaying 9-path quasi-static Rayleigh fading		
Receive channel state inf.	Perfect		
Decoding algorithm	MLD	MLSE	

## 3. Proposed MU-C-MIMO-OFDM system

Figure 5 shows the system block diagram of the proposed MU-C-MIMO-OFDM system. Based on C-MIMO-OFDM described in Section 2, MU-MIMO architecture is added, and the multiuser transmission is achieved. Each user has a different key  $\mathbf{g}_{M,0}$  from the others but shares it only with the transmitter. Consequently, a secure transmission with a channel coding gain for each user is obtained.

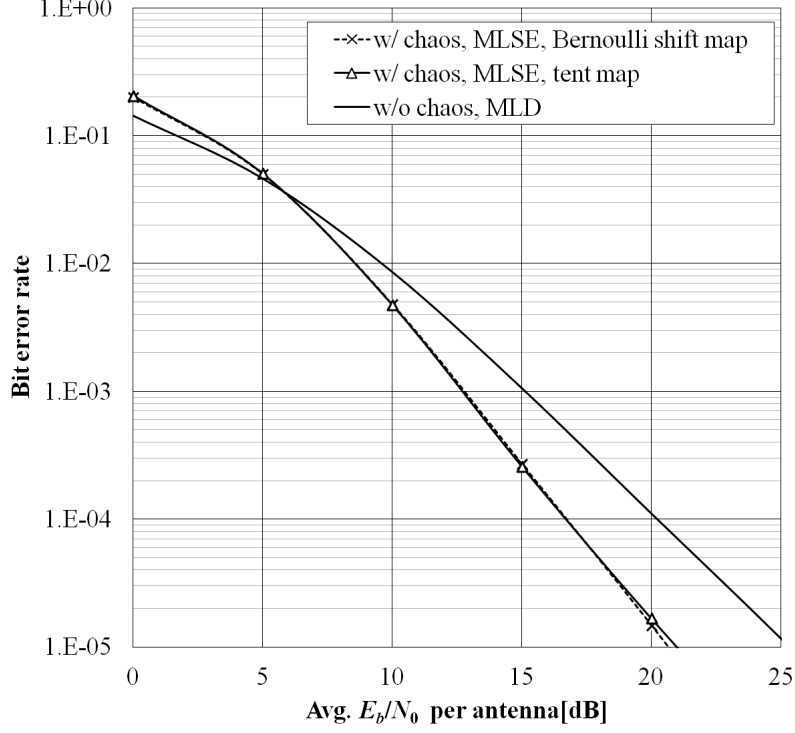


Fig. 4. BER Performance of chaos MIMO-OFDM.

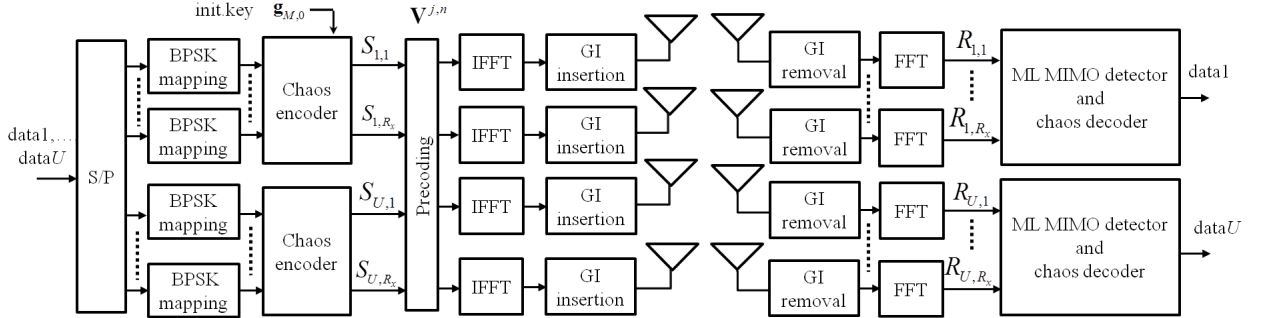


Fig. 5. System block diagram of proposed multiuser chaos MIMO-OFDM.

### 3.1 Transmitter and receiver design

Consider the downlink MU-C-MIMO-OFDM. Let  $U$  be the number of users ( $1 \leq k' \leq U$ ),  $R'_x$  be the number of receive antennas per user, and  $T_x = UR'_x$  be the number of transmit antennas. Then, the transmit sequence  $\mathbf{S}^{j,n}$  in the  $j$ -th block at the  $n$ -th subcarrier is defined by

$$\begin{aligned} \mathbf{S}^{j,n} &= [S_{1,1} \cdots S_{1,R'_x} \cdots S_{k',1} \cdots S_{k',R'_x} \cdots S_{U,1} \cdots S_{U,R'_x}]^T \\ &= [(\mathbf{S}_1^{j,n})^T \cdots (\mathbf{S}_{k'}^{j,n})^T \cdots (\mathbf{S}_U^{j,n})^T]^T \end{aligned}$$

where  $S_{k',1}$  is the transmit symbol to the first receive antenna of the  $k'$ -th user, and the vector  $\mathbf{S}_{k'}^{j,n}$  is the transmit sequence to user  $k'$  as

$$\mathbf{S}_{k'}^{j,n} = [S_{k',1} \cdots S_{k',R'_x}]^T$$

The receive sequence of the  $k'$ -th user is defined by

$$\mathbf{R}_{k'}^{j,n} = [R_{k',1} \cdots R_{k',R'_x}]^T$$

and the sequence of all users  $\mathbf{R}_{k'}^{j,n}$  is given by

$$\begin{aligned} \mathbf{R}^{j,n} &= [(\mathbf{R}_1^{j,n})^T \cdots (\mathbf{R}_{k'}^{j,n})^T \cdots (\mathbf{R}_U^{j,n})^T]^T \\ &= [R_{1,1} \cdots R_{1,R'_x} \cdots R_{k',1} \cdots R_{k',R'_x} \cdots R_{U,1} \cdots R_{U,R'_x}]^T \end{aligned}$$

Then,  $\mathbf{R}^{j,n}$  is obtained by

$$\mathbf{R}^{j,n} = \mathbf{H}^{j,n} \mathbf{V}^{j,n} \mathbf{S}^{j,n} = \tilde{\mathbf{H}}^{j,n} \mathbf{S}^{j,n} \quad (15)$$

where  $\mathbf{V}^{j,n}$  is a precoding matrix in the  $j$ -th block at the  $n$ -th subcarrier, and  $\tilde{\mathbf{H}}^{j,n}$  is a block diagonal matrix. By multiplying the precoding matrix  $\mathbf{V}^{j,n}$  by the transmit vector  $\mathbf{S}^{j,n}$ , the inter-user interference is eliminated. The derivation of  $\mathbf{V}^{j,n}$  is described in the next subsection. Equation (15) can be described in matrix form as

$$\begin{bmatrix} \mathbf{R}_1^{j,n} \\ \vdots \\ \mathbf{R}_{k'}^{j,n} \\ \vdots \\ \mathbf{R}_U^{j,n} \end{bmatrix} = \begin{bmatrix} \tilde{\mathbf{H}}_1^{j,n} & & & \mathbf{0} \\ & \ddots & & \\ & & \tilde{\mathbf{H}}_{k'}^{j,n} & \\ & & & \ddots \\ \mathbf{0} & & & & \tilde{\mathbf{H}}_U^{j,n} \end{bmatrix} \begin{bmatrix} \mathbf{S}_1^{j,n} \\ \vdots \\ \mathbf{S}_{k'}^{j,n} \\ \vdots \\ \mathbf{S}_U^{j,n} \end{bmatrix} \quad (16)$$

$$\mathbf{R}_{k'}^{j,n} = \tilde{\mathbf{H}}_{k'}^{j,n} \mathbf{S}_{k'}^{j,n}$$

where  $\tilde{\mathbf{H}}_{k'}^{j,n}$  is an  $R'_x \times R'_x$  equivalent channel matrix for user  $k'$ .

### 3.2 Derivation of precoding matrix

First, a  $T_x \times R'_x$  precoding matrix  $\hat{\mathbf{V}}_{k'}^{j,n}$  for the  $k'$ -th user in the  $j$ -th block in the  $n$ -th subcarrier is derived [9, 10]. When  $\mathbf{H}_{k'}^{j,n}$  is an  $R'_x \times T_x$  channel matrix between the transmitter and the  $k$ -th user,  $\hat{\mathbf{V}}_{k'}^{j,n}$  has to satisfy

$$\mathbf{H}_k^{j,n} \hat{\mathbf{V}}_{k'}^{j,n} = \mathbf{0} \quad , \quad (k' \neq k)$$

Next, a  $(U-1)R'_x \times T_x$  subchannel matrix of all users except the  $k'$ -th user is defined by

$$\hat{\mathbf{H}}_{k'}^{j,n} = [(\mathbf{H}_1^{j,n})^T \cdots (\mathbf{H}_{k'-1}^{j,n})^T (\mathbf{H}_{k'+1}^{j,n})^T \cdots (\mathbf{H}_U^{j,n})^T]^T$$

Then, when  $\hat{\mathbf{H}}_{k'}^{j,n}$  is decomposed to singular values, we obtain

$$\hat{\mathbf{H}}_{k'}^{j,n} = \hat{\mathbf{U}}_{k'}^{j,n} \hat{\mathbf{D}}_{k'}^{j,n} (\hat{\mathbf{V}}_{k'}^{j,n})^H \quad (17)$$

where  $\hat{\mathbf{U}}_{k'}^{j,n}$  and  $\hat{\mathbf{V}}_{k'}^{j,n}$  are  $(U-1)R'_x \times (U-1)R'_x$  and  $T_x \times T_x$  unitary matrices, respectively, and  $\hat{\mathbf{D}}_{k'}^{j,n}$  is a  $(U-1)R'_x \times T_x$  diagonal matrix whose diagonal and non-diagonal elements are the square roots of the eigenvalues of  $(\hat{\mathbf{V}}_{k'}^{j,n})^H \hat{\mathbf{V}}_{k'}^{j,n}$  and zero, respectively. Here,  $H$  denotes the Hermitian transpose, and the column vectors of  $\hat{\mathbf{D}}_{k'}^{j,n}$  from  $(U-1)R'_x$  to  $T_x$  become zero vectors. From (17),  $\hat{\mathbf{H}}_{k'}^{j,n}$  satisfies

$$\hat{\mathbf{H}}_{k'}^{j,n} \hat{\mathbf{V}}_{k'}^{j,n} = \hat{\mathbf{U}}_{k'}^{j,n} \hat{\mathbf{D}}_{k'}^{j,n} \quad (18)$$

and when the column vectors from  $(U-1)R'_x + 1$  to  $T_x$  of the left term in (18) are extracted, we obtain

$$\begin{bmatrix} \mathbf{H}_1^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}((U-1)R'_x + 1) & \cdots & \mathbf{H}_1^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}(T_x) \\ & \ddots & \\ \mathbf{H}_{k'-1}^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}((U-1)R'_x + 1) & \cdots & \mathbf{H}_{k'-1}^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}(T_x) \\ \mathbf{H}_{k'+1}^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}((U-1)R'_x + 1) & \cdots & \mathbf{H}_{k'+1}^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}(T_x) \\ & \ddots & \\ \mathbf{H}_U^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}((U-1)R'_x + 1) & \cdots & \mathbf{H}_U^{j,n} \hat{\mathbf{v}}_{k'}^{j,n}(T_x) \end{bmatrix} = \mathbf{0} \quad (19)$$

where  $\hat{\mathbf{v}}_{k'}^{j,n}(i)$  is the  $i$ -th column vector of  $\hat{\mathbf{V}}_{k'}^{j,n}$ . It is confirmed from (19) that the column vectors from  $(U-1)R'_x$  to  $T_x$  of  $\hat{\mathbf{V}}_{k'}^{j,n}$  form a null space for all users other than user  $k$ . Therefore, the precoding matrix of the  $k'$ -th user  $\hat{\mathbf{V}}_{k'}^{j,n}$  of  $T_x \times R'_x$  is given by

$$\hat{\mathbf{V}}_{k'}^{j,n} = (\hat{\mathbf{v}}_{k'}^{j,n}((U-1)R'_x + 1) \hat{\mathbf{v}}_{k'}^{j,n}((U-1)R'_x + 2) \cdots \hat{\mathbf{v}}_{k'}^{j,n}(T_x))$$

and finally a comprehensive precoding matrix  $\mathbf{V}^{j,n}$  for all users is composed as follows:

$$\mathbf{V}^{j,n} = (\hat{\mathbf{V}}_1^{j,n} \hat{\mathbf{V}}_2^{j,n} \cdots \hat{\mathbf{V}}_U^{j,n})$$



### 3.3 Decoding of MU-C-MIMO-OFDM

The decoding algorithm of MU-C-MIMO-OFDM is almost the same as (9), except for the channel matrix in creating the symbol replica. The  $k'$ -th user conducts the MLSE decoding by

$$\hat{\mathbf{S}}_{k'}^j = \arg \min_{\mathbf{s}_{k'}^j} \sum_{q=0}^{B-1} \|\mathbf{R}_{k'}^{j,q} - \tilde{\mathbf{H}}_{k'}^{j,n} \mathbf{s}_{k'}^{j,q}\| \quad (20)$$

Here,  $\hat{\mathbf{S}}_{k'}^j$  is the transmit block of the  $k'$ -th user in the  $j$ -th block, and  $\tilde{\mathbf{S}}_{k'}^j$  is the decoded block.

## 4. Numerical results

### 4.1 Performances with identically distributed user channel

The performances of the proposed schemes were evaluated by computer simulations under the conditions in Table II. It is assumed that the channels are assumed to be i.i.d 1-dB decaying 9-path quasi-static Rayleigh fading channels in terms of each antenna and MIMO-OFDM block and that the channels are perfectly known to all receivers. The block length is four, and the numbers of users are 1, 2, 4, and 8. Each user has a different chaos initial key, which is shared only with the transmitter. In addition, to obtain the average performance, the initial keys are randomly changed at each block. Figure 6 shows the BER performances decoded by the MLSE of (20) at each block. It is shown that the BER of the proposed scheme is improved for the conventional unencrypted MIMO with a maximum likelihood decoding (MLD) with an average Eb/N0 over 5 dB, regardless of the number of users. However, it is noted that the decoding complexity is increased in the proposed scheme because of the block decoding. It is also found that the BER becomes 0.5 when the initial key is not identical (denoted as ‘unsync’ in Fig. 6), that is, physical layer security is ensured for every user.

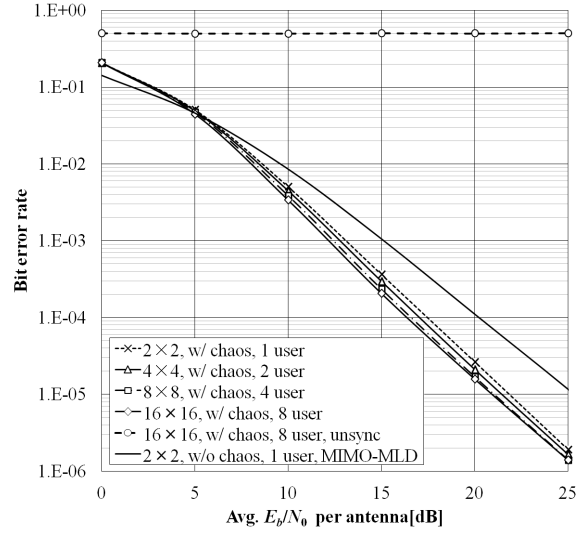
**Table II.** Simulation conditions.

	Conventional scheme	Proposed scheme
Modulation	BPSK	
Num. of 1OFDM symbols	64	
Num. of transmit antenna $T_x$	2	2,4,8, 16
Num. of receive antenna per user $R'_x$	2	
Num. of users $U$	1	1,2,4, 8
Chaos	N/A	Bernoulli shift map
Num. of MIMO symbols on 1 block $B$	N/A	4
Num. of chaos signals $M$	N/A	10
Num. of chaos iteration $BO$	N/A	19
Channel	1-dB decaying 9-path quasi-static Rayleigh fading	
Receive channel state inf.	Perfect	
Decoding algorithm	MLD	MLSE

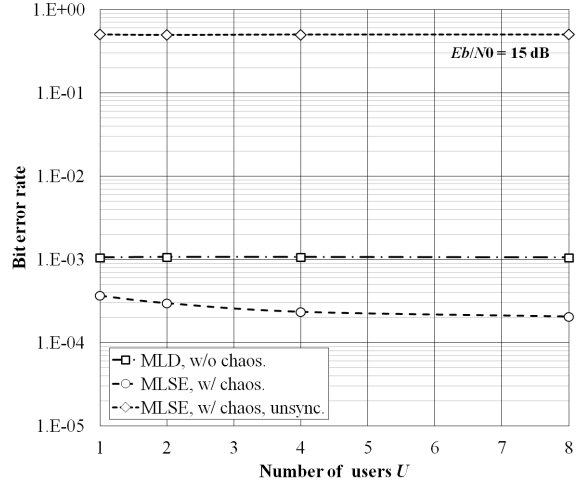
Figure 7 shows the BER performance versus the number of users at an average Eb/N0 of 15 dB. Figures 6 and 7 show that the BER slightly improves according to the increase in the number of users. In MIMO-OFDM, if the channel coding is used in the frequency direction, BER is improved because of the frequency diversity effect. When the number of delay paths and the delay spread is increased, the frequency diversity effect is enlarged, and the performance is further improved. In the proposed scheme, this effect happens according to the increase in the number of users. Because the frequency diversity is obtained by the channel coding function of C-MIMO, the BER is improved compared to MIMO-MLD regardless of  $U$ . Furthermore, as shown in Fig. 8, the equivalent channel ( $\tilde{\mathbf{H}}_{k'}^{j,n}$  of (16)) is changed according to the number of users.

Figure 8 is calculated from the ensemble average of the squared impulse response transformed from one subcarrier channel of an OFDM channel matrix  $\tilde{\mathbf{H}}_{k'}^{j,n}$  in the frequency domain. We can see that the delay spread effect is enlarged according to the increase in the number of users. Thus, as a result, a strong frequency diversity effect is obtained, and the BER is improved in proportion to the number

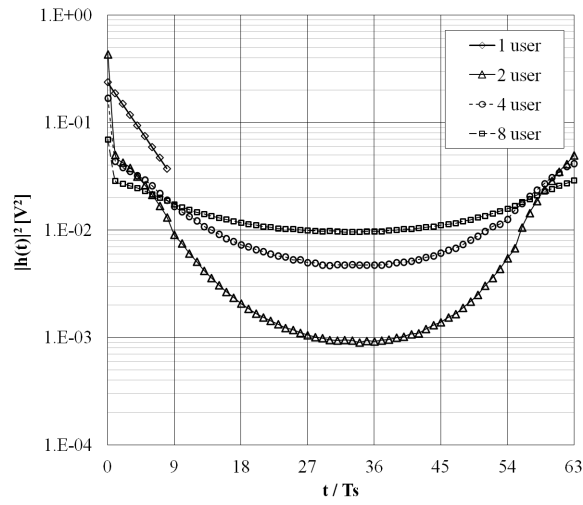




**Fig. 6.** BER performance comparison of single-user and multiuser MIMO in downlink.



**Fig. 7.** BER performance versus number of users at  $E_b/N_0 = 15$  dB.



**Fig. 8.** Average squared impulse response of  $\tilde{\mathbf{H}}_{k'}^{j,n}$  in time domain.

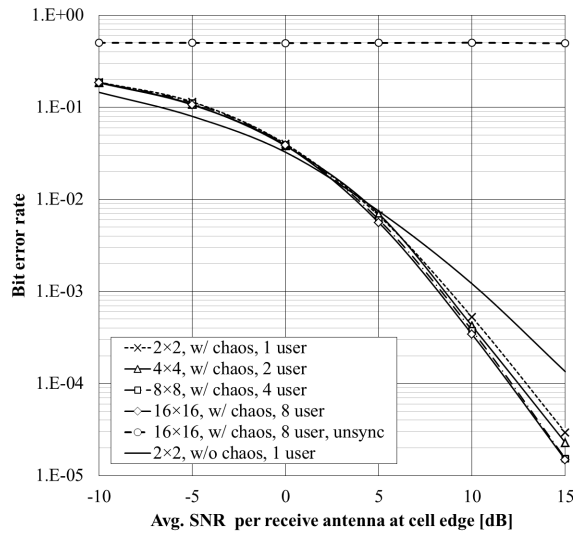
of users. When the number of antennas is increased, antenna diversity is usually obtained. This effect is the same as that shown in Fig. 8. Note that the computational complexity of precoding in the transmitter increases as  $O(n^3)$  as the number of users  $n$  increases [11].

## 4.2 Performances with Non-identically distributed user channel

In addition to the conditions in Table II, the path loss and shadowing parameter were considered, as shown in Table III, and a simulation was conducted. It was assumed that each user was equally and randomly distributed within a single circle cell whose radius was normalized to 1. Figure 9 shows the average BER performance versus the average SNR per receive antenna at a cell edge user using the MLSE of (20). It was found that the channel coding effect was achieved compared to single-user MIMO, and frequency diversity in proportion to the number of users is still obtained even when the user location is distributed. The reason for this is the same as what was stated in Subsection 4.1.

**Table III.** Channel parameters of path loss and shadowing.

Path loss exponent $\alpha$	3.5
Standard deviation of Shadowing loss $\beta$ [dB]	7



**Fig. 9.** BER performance comparison of single-user and multiuser MIMO considering propagation loss in downlink.

## 4.3 Security evaluation of MU-C-MIMO-OFDM

### 4.3.1 Information theoretic security

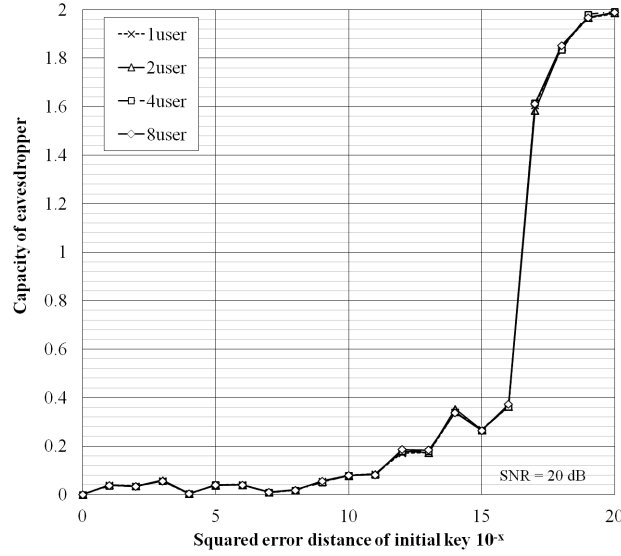
In general, the safety of wireless communications is evaluated from the information theoretical or computational point of view. First, the information theoretic security is considered. The information theoretic security can be evaluated by the channel capacity of an eavesdropper [12]. When the channel is an i.i.d. Rayleigh fading channel, the equivalent channel can be modeled as a binary symmetric channel (BSC), and the channel capacity of an eavesdropper  $C_R$  is calculated by

$$C_R = R_x[1 + P_{eR} \log P_{eR} + (1 - P_{eR}) \log(1 - P_{eR})] \quad (21)$$

where  $P_{eR}$  is the bit error rate of the eavesdropper. The communication can be recognized as safe when  $C_R$  is near zero.

In MU-MIMO transmission, beamforming is conducted at the transmitter based on the feedback channel state information (CSI) from legitimate users. When the eavesdropper pretends to be a legitimate user and sends his CSI, the data for the legitimate user are transmitted to the eavesdropper.

However, in MU-C-MIMO-OFDM, the data cannot be decoded unless the eavesdropper has the initial key  $\mathbf{g}_{M,0}$  of the legitimate user. Thus, it is assumed that the eavesdropper obtained a close key in terms of the squared Euclidean distance by any means and that decoding was attempted. The security of this case was evaluated by a computer simulation. The channel capacity of the eavesdropper is calculated under the conditions in Tables II and III, and the average SNR for the cell edge user is 20 dB. The results in Fig. 10 show that the security is ensured when the difference in the key distance is more than  $10^{-11}$ , which is quite small, and that the security is the same as that of single-user C-MIMO. Consequently, the proposed scheme provides the secure multiuser transmission.



**Fig. 10.** Channel capacity of eavesdropper versus squared Euclidean distance from correct key when SNR of cell edge user is 20 dB.

#### 4.3.2 Computational security

To evaluate the computational security, the number of decoding search patterns in the MU-C-MIMO-OFDM scheme is calculated. The secret key of the proposed scheme

$$\mathbf{g}_{M,0} = (g_{00}, \dots, g_{0(M-1)})$$

has  $M$  complex values. Then, when the 64-bit double floating-point value is used in the transmitter and the receiver, the secret key becomes  $128 \times M$  bits long, so the eavesdropper needs  $2^{128M}$  trials to decode it. Furthermore, when the number of transmit antennas and the block length are  $T_x = 2$  and  $B = 4$ , respectively, the number of multiplication operations in MLSE decoding becomes 6,144. Hence, the total number of decoding calculations is

$$6144 \times 2^{128M} \cong 10^{38.5M+3.79}$$

If a reference PC with a processing speed of  $4.4 \times 10^9$  [FLOPS/sec] is used for the security evaluation [13], decoding requires

$$10^{38.5M+3.79} / (4.4 \times 10^9 \times 31536000) \cong 10^{38.5M-13.4} [\text{years}]$$

Compared with the upper layer protocol of RSA-2048, which requires  $25 \times 10^{16}$  years for decoding, the above complexity of the proposed scheme with  $M = 10$  can be recognized as sufficiently safe.

## 5. Conclusions

In this paper, we extended a chaos MIMO-OFDM scheme to a multiuser MIMO system and proposed a multiuser chaos MIMO-OFDM scheme with physical layer security for every user and channel coding

gain. According to the increase in the number of users, the frequency diversity effect was enlarged, and the BER performance of the proposed scheme was improved in the cases of undistributed and distributed users. In addition, security was evaluated by the leak capacity with close initial keys, and the robustness of the proposed scheme was confirmed.

## Acknowledgments

This work is partially supported by Strategic Information and Communications R&D Promotion Programs (SCOPE) in the Ministry of Internal Affairs and Communications, Adaptable and Seamless Technology Transfer Program through the target-driven R&D, JST, and KDDI foundation. The authors wish to thank these entities for their support.

## References

- [1] F. Yu, C. Tellambura, and W.A. Krzymien, "Limited-feedback precoding for closed-loop multiuser MIMO OFDM systems with frequency offsets," *IEEE Trans. Commun.*, vol. 7, no. 11, pp. 4155–4165, November 2008.
- [2] R. Holakouei, A. Silva, and A. Gameiro, "Transmit power allocation for precoded distributed MIMO OFDM systems," *IEEE International Conference on Advanced Information Networking and Applications (AINA) 2010*, pp. 190–197, April 2010.
- [3] W.W.L. Ho and Y.C. Liang, "Optimal resource allocation for multiuser MIMO-OFDM systems with user rate constraints," *IEEE Trans. Vehicular Tech.*, vol. 58, no. 3, pp. 1190–1203, March 2009.
- [4] M. Schellmann, T. Haustein, and V. Jungnickel, "Spatial transmission mode switching in multiuser MIMO-OFDM systems with user fairness," *IEEE Trans. Vehicular Tech.*, vol. 59, no. 1, pp. 235–247, March 2010.
- [5] M. Benjillali and L. Szczecinski, "Quantization of channel state information for detect-and-forward relaying schemes," *Proc. 2009 IEEE Global Telecommunications Conference (GLOBECOM 2009)*, Hawaii, December 2009.
- [6] E. Okamoto, "A chaos MIMO transmission scheme for channel coding and physical-layer-security," *IEICE Trans. Commun.*, vol. E95-B, no. 4, April 2012.
- [7] E. Okamoto, "Chaos MIMO-OFDM transmission scheme achieving physical-layer security in mobile channel environments," *IEICE Technical Report*, vol. 112, no. 239, RSC2012-125, pp. 1–6, October 2012.
- [8] E. Okamoto, "A secure cooperative relay transmission using chaos MIMO scheme," *International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 374–378, July 2012.
- [9] S. Umeda, S. Suyama, H. Suzuki, and K. Fukawa, "PAPR Reduction Method for Block Diagonalization in Multiuser MIMO-OFDM Systems," *IEEE Vehicular Technology Conference (VTC 2010-Spring)*, pp. 1–5, May 2010.
- [10] R. Holakouei, A. Silva, and A. Gameiro, "Precoded multiuser distributed MIMO OFDM systems," *IEEE Intl. Symp. on Wireless Communication Systems (ISWCS) 2009*, pp. 605–608, September 2009.
- [11] Y. Wang, K. Cunningham, P. Nagvajara, and J. Johnson, "Design and prototype of singular value decomposition hardware in IEEE 802.11n MIMO standards for software defined radio," *International Conference on ReConFigurable Computing and FPGAs*, pp. 400–405, December 2010.
- [12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *Proc. Int'l Sym. on Information Theory (ISIT)*, pp. 524–528, July 2008.
- [13] T. Kleinjung, "Evaluation of complexity of mathematical algorithms," *CRYPTREC technical report No. 0604 in FY2006*, 2007.