Horiike et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:205
https://doi.org/10.1186/s13638-018-1156-8

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A downlink non-orthogonal multiple access scheme having physical layer security

Naoto Horiike[1*], Eiji Okamoto[1*] and Tetsuya Yamamoto[2]

Abstract

In recent years, the standardization for the fifth generation (5G) mobile communication systems has been actively discussed, and it is expected that a large number of wireless communication terminals, and beyond, in the current systems are accommodated in 5G systems. One of the steps in establishing this system is an advanced multiple access technology. In this paper, we propose a chaos non-orthogonal multiple access (C-NOMA) scheme for downlink transmission that offers high capacity allocation and secure wireless multiple access with physical layer security. In 5G systems where many terminals concurrently communicate, it is also important to ensure communication integrity for each user while maintaining large capacity communication. As a secure wireless channel-coded communication scheme, we have proposed a chaos multiple-input multiple-output (C-MIMO) scheme using the principle of chaos communication. By applying C-MIMO into a power-domain non-orthogonal multiple access transmission, we were able to demonstrate the operation and suitability of the C-NOMA configuration for handling both large capacity and physical layer security against eavesdroppers. We also demonstrated its improved performances through numerical simulations, and provided comparisons with those of conventional NOMA and chaos orthogonal frequency division multiple access schemes. In addition, we evaluated the security capability of the proposed technique based on the channel capacity of eavesdroppers and showed that secure transmission can be achieved using floating-point calculations.

Keywords: 5G, Downlink, Non-orthogonal multiple access, Chaos, Physical layer security

1 Introduction

With the increasing advancement of Internet technology, and in addition to conventional physical devices such as personal computers and smartphones, all kinds of other objects around the world like household appliances and automobiles are being connected to the Internet. The number of these terminals is explosively *rising*, and according to a survey by IHS Technology, the number of Internet of Things (IoT) devices as of 2016 is estimated to be around 17.3 billion, which is incidentally about 13% higher than the figures presented in 2015 by a similar survey. In addition, it is expected that the number of IoT devices will expand to about 300 million worldwide in 2020, which is twice as much as the current figures. Wireless communication technologies are indispensable in the integration of the many existing terminals in various places, into the same network; however, at the same time, a massive surge in wireless traffic volume also presents a perplexing problem. Wireless traffic in 2020, along with the general adoption of smartphones, is expected to be nearly 100 times than that in 2010. Hence, there is an increasing demand for further capacity enhancement of wireless communication systems, and the fifth generation (5G) mobile communication system has been rapidly developed to meet these demands [1–3]. The accommodation of mobile phones, automobiles, and IoT devices is planned for 5G scenarios. To ensure that this objective is achieved, the enhanced capabilities of the peak rate, massive connectivity, and ultra-reliable low latency will need to be actualized. Thus, 5G is expected to act as a social infrastructure in the information and communication technology (ICT) society, which will be further advanced in the future.

One of the key technologies for implementing high capacity allocation is an advanced multiple access scheme. In current mobile communication systems such as long-term

* Correspondence: n.horiike.027@nitech.jp; okamoto@nitech.ac.jp
[1]Graduate School of Engineering, Nagoya Institute of Technology, Nagoya, Aichi, Japan
Full list of author information is available at the end of the article

evolution (LTE) and advanced LTE, the orthogonal frequency division multiple access (OFDMA) scheme is adopted as a downlink, in which the principle of orthogonal frequency division multiplexing (OFDM) is applied for multiuser access [4]. In an OFDMA setup, one user is assigned to one channel in the frequency domain and user signals are densely deployed to improve the frequency efficiency. The system capacity can be increased in OFDMA by exploiting the multiuser diversity effect, where good channels are selectively allocated to each user. However, the orthogonal multiple access scheme cannot accommodate the enormous amount of today's wireless traffic, and as such, further evolution is required. Consequently, in 5G standardization, a non-orthogonal multiple access (NOMA) scheme that allows non-orthogonal frequency resource allocation and assigns multiple users to a single channel has been proposed [5, 6]. In a NOMA scheme, a power domain is utilized in addition to the frequency domain for user multiplexing, and a higher system capacity than the OFDMA configuration can be obtained by allowing a multiuser superimposed type of allocation for the inter-user interference.

However, in wireless communication environments where a large number of terminals exist in an assumed 5G scenario, and a large amount of information is simultaneously exchanged, wireless security for each transmission is equally important. In other words, it is important to ensure confidentiality by encryption to prevent information from leaking to third parties and eavesdroppers during wireless transmissions. In current communication systems, upper layer encryption protocols such as public key cryptography are mainly used. However, the enhancement of encryption properties only in the upper layer often leads to protocol complications and an increase in calculation complexity. Therefore, ensuring the integrity of wireless communication only in the upper layer is not desirable, but a similar approach in the physical layer where the modulated signal is encrypted is also effective. The physical layer encryption can enhance security protocols when it is concurrently used with the upper layer encryption, or can, otherwise, simplify the upper layer security protocol. As with regards to physical layer security schemes, we have proposed a chaos multiple-input multiple-output (C-MIMO) transmission method, which has both the functionality of encrypted modulation and channel coding, for exploiting the principle of chaos communications [7]. In this method, Gaussian modulated signals are generated from chaos signals correlated with transmission bits in a short block, and these signals are transmitted by MIMO spatial multiplexing. A chaos signal is irregular and unpredictable, but its behavior is deterministically controlled by the initial chaos value. By taking advantage of this feature, the initial chaos value can be used as a signal key shared by the transmitter and receiver in the C-MIMO system, thereby achieving the physical layer encryption effect based on common key encryption. In essence, only a valid user at the receiver end who has the same signal key used in the transmitter can correctly decode the received signals, thus blocking out third party intrusions. In addition, C-MIMO has a channel coding effect at a coding rate of 1 by convoluting the transmission bit to the chaos signal in generating the transmission signal. Thus, C-MIMO can provide secure and high-quality wireless transmission. However, C-MIMO is a link transmission scheme, and has not been applied for high-capacity allocation multiple access technologies such as 5G.

In this paper, we propose a chaos NOMA (C-NOMA) transmission scheme capable of providing large capacity and secure multiuser access in the physical layer, where the principle of C-MIMO is applied to the NOMA transmission scheme [8]. (Comments #1–1, #1–4, #2–2, #3–6) More specifically, in this study, a downlink power-domain superposition NOMA is investigated, and the principle of C-MIMO is applied to it. Recently, secure downlink NOMA schemes have been actively studied [9–14]. In [9, 10], secure beamforming schemes in multiple-input single-output (MISO)- and MIMO-NOMA were proposed, where a cell-edge user is recognized as a potential eavesdropper. In [11, 12], secrecy rate maximization problems in single-input single-output (SISO)- and MIMO-NOMA were respectively presented. The physical layer security of NOMA in large-scale networks has been studied in [13]. In [14], the security rate in unicast and multicast streaming scenarios in NOMA was investigated. In these studies, secrecy of the system is safeguarded in the physical layer using SISO, MISO, or MIMO channel matrix and beamforming techniques like the multi-user MIMO system, in which user-specific components are not accommodated. Furthermore, the security is based on the information-theoretic security, and there exists some conditions on eavesdroppers such as user location in order to obtain the security rate. On the other hand, in our proposed C-NOMA, the security is based on the computational security, which is a practical approach, and user-specific key signals are used for secure transmission, which does not rely on channel state information (CSI). Moreover, eavesdroppers need to estimate the key signal for the received target signals, which consequently requires a huge amount of calculation. Thus, strong confidentiality is required based on this computational security. In addition, very reliable wireless communication can be conducted with the channel coding effect of C-MIMO. The contributions of this study are as follows: (1) the secure transmission of NOMA is analyzed in terms of computational security, (2) no limiting condition is needed for eavesdroppers, and (3) channel coding effect is effectively obtained. Thus, the proposed C-NOMA scheme can provide secure and very reliable transmission in cellular environments assumed in 5G. We demonstrated the improved performance of the C-NOMA configuration via numerical simulations and compared them to those of conventional unencrypted NOMA and chaos OFDMA (C-OFDMA) encrypted schemes [15]. It is shown also that the coding gain and physical layer security effect can be obtained without degradation of transmission efficiency in the proposed method for conventional unencrypted NOMA scheme. Furthermore, the maximum throughput increases in the proposed technique compared to the conventional C-OFDMA setup. The security properties for ensuring secure connections against eavesdroppers are also evaluated for the C-NOMA scheme based on the equivalent channel capacity of an eavesdropper.

This paper is organized as follows: in Section 2, the system model of a downlink chaos NOMA scheme is described, and the chaos modulation, demodulation, and NOMA user scheduling in the proposed system are explained. Section 3 presents the numerical results and performance comparisons for conventional schemes. Finally, conclusive remarks are given in Section 4.

(Comments #3–5) Notations: in the following section, lowercase and uppercase boldface letters denote vectors and matrices, respectively.

2 Proposed downlink chaos NOMA system

In the proposed scheme, we assume a downlink NOMA transmission system from base station (BS) to each user equipment (UE) in a single-cell environment, in which transmission signals are superimposed in the power domain. Additional file 1: Figure S1 shows the system model of the downlink NOMA scheme, where no more than two users are superimposed into one subcarrier (i.e., the maximum number of superimposing users is $m_s = 2$). In this system, the BS selects either orthogonal multiple access (OMA) or NOMA transmission at each subchannel based on the *CSI* sent from each UE. Moreover, this system utilizes MIMO type of transmission in which the BS and each UE have multiple antennas. The signal processing at the BS and UE is described as follows:

2.1 Structure of base station

Additional file 2: Figure S2 shows the block diagram of the base station transmitter of the C-NOMA scheme. At the BS, chaos-modulated signals for all K users in a certain cell are superimposed in the power domain in each subchannel in the frequency domain based on a scheduling algorithm described later in Section 2.1.1. The superimposed signals are transmitted via N_t MIMO transmission antennas after the application of inverse fast Fourier transform (IFFT), and the addition of a guard interval (GI).

2.1.1 Chaos modulation

The chaos modulation of N_u bit sequence for user u ($1 \le u \le K$) is described in this section [7]. In the chaos modulation, N_u bits are divided into short bit sequences $\mathbf{b}_n(u)$ consisting of N_tB bits, and the

$$\mathbf{b}_n(u)=\left\{b_{n,0},\dots,b_{n,N_tB-1}\right\}\ b_{n,m}\in\{0,1\} \tag{1}$$

modulation is conducted for each short sequence. N_t is the number of transmission antennas at the BS, B is the MIMO block length, and the nth short bit sequence is given as
where the block index n is $0 \le n \le N_u/(N_tB) - 1$, and the bit index m is $0 \le m \le N_tB - 1$. In addition, the chaos modulation uses a user-specific key signal for encryption. A complex symbol $c_0(u)$ of user u is defined as the signal key:

$$0 < \operatorname{Re}[c_0(u)] < 1, 0 < \operatorname{Im}[c_0(u)] < 1 \tag{2}$$

In practical systems, it is assumed that this key symbol is generated from the unique ID of each UE hardware. However, in this study, it is generated using pseudo uniform and real random number with 32-bit precision in the real and imaginary parts, respectively. In downlink transmissions, the BS holds the key signals of all accommodated users for conducting chaos modulation. The chaos modulation is executed by $c_0(u)$ and $\mathbf{b}_n(u)$ for user u. First, an initial modulated value for chaos generation x_0 is composed according to the following rule:

$$x_0 = \begin{cases} a & \left(b_{n,m} = 0\right) \\ 1-a & \left(b_{n,m} = 1, a > 0.5\right) \\ a + 0.5 & \left(b_{n,m} = 1, a \le 0.5\right) \end{cases} \tag{3}$$

$$\begin{aligned} &\text{Real part} : a = \operatorname{Re}\left[c_{(k-1)}(u)\right], m = k-1 \\ &\text{Imaginary part} : a = \operatorname{Im}\left[c_{(k-1)}(u)\right],\ m = k \mod (N_tB) \end{aligned} \tag{4}$$

The above operation is conducted in the real and imaginary parts of $c_{(k-1)}(u)$, respectively (comment #3–1), that is, each part is individually modulated. Different bits are also convoluted in these complex component parts based on Eq. (4) in the range of $1 \le k \le N_tB$. When $k = 1$, the key signal $c_0(u)$ is used. (Comment #3–1) For example, when $k = 1$, the real and imaginary parts of $c_0(u)$ are modulated by $b_{n,\ 0}$ and $b_{n,\ 1}$, respectively, using Eqs. (3) and (4). Similarly, the third and fourth bits $b_{n,\ 2}$, $b_{n,\ 3}$ are correlated to $c_1(u)$. Thus, in this process, the convolutional operation is conducted and the channel coding effect is produced at a coding rate of 1. Next, the chaos signal is generated from the initial value x_0 by using chaos generation equation. In this study, Bernoulli shift map is adopted and given as

$$x_{l+1} = 2x_l \mod 1, \tag{5}$$

where l is the iteration index. With this iterative operation, an irregular chaos modulated signal is deterministically generated from the initial variable x_0. Therefore, C-NOMA is a common key encryption scheme that utilizes the deterministic characteristics of chaos, and the modulated signals can be correctly demodulated only when the transmitter and receiver share the exact same key $c_0(u)$. It has been reported that the chaos signal converges to zero with finite resolution [16, 17]. To avoid these zero convergences, Eq. (5) is modified slightly from mod 1 to mod $(1 - 10^{-11})$ to calculate the double floating point in the numerical simulation. Following this step, the processed chaos signal obtained after the iteration of Eq. (5) is extracted as elements of complex modulated signal $c_k(u)$ using the following equation:

$$\begin{aligned}\text{Real part}: \ \mathrm{Re}[c_k(u)] &= x_{\left[\ Ite+b_{(k+N_\mathrm{t}B/2)} \mod (N_tB)\ \right]}\\ \text{Imaginary part}: \ \mathrm{Im}[c_k(u)] &= x_{\left[\ Ite+b_{(k+N_\mathrm{t}B/2+1)} \mod (N_tB)\ \right]}\end{aligned} \tag{6}$$

where Ite is a base chaos iteration number and the subscript of x in Eq. (6) corresponds to the chaos iteration number l in Eq. (5). This complex chaotic signal $c_k(u)$ is not only used as the modulated signal to be transmitted, but also reapplied in Eq. (4) for generating the next modulation signal as a convolutional coded modulation. By adding the different transmission bits into the chaos iteration number and changing the repetition number of Eq. (5), Eq. (6) can increase the randomization of $c_k(u)$ and extend the average squared Euclidean distance among neighboring signals. Then, from the extracted chaos signals, transmission Gaussian symbols are generated using Box-Muller transform [18]. The m_2th$(0 \leq m_2 \leq N_\mathrm{t}B - 1)$transmission symbol correlated with the nth transmission bit sequence $\mathbf{b}_n(u)$ is given as

$$s_{n,m_2} = \sqrt{-2\ \ln\left(c_x^{(k)}\right)}\left\{\ \cos\left(2\pi c_y^{(k)}\right) + j\ \sin\left(2\pi c_y^{(k)}\right)\right\}\cdot\sigma + \mu \tag{7}$$

where $c_x^{(k)}$ and $c_y^{(k)}$ are the uniformly distributed symbols generated from the following equations:

$$c_x^{(k)} = \frac{1}{\pi}\cos^{-1}[\ \cos\{37\pi(\ \mathrm{Re}[c_k(u)] + \ \mathrm{Im}[c_k(u)])\}] \tag{8}$$

$$c_y^{(k)} = \frac{1}{\pi}\sin^{-1}[\ \sin\{43\pi(\ \mathrm{Re}[c_k(u)]- \ \mathrm{Im}[c_k(u)])\}] + \frac{1}{2}$$

Equation (8) is used to generate two quasi-independent uniform random symbols from chaos signals. In this paper, the mean and standard deviation are $\mu = 0$ and $\sigma = 1/\sqrt{2}$, respectively, as obtained using Eq. (7). These formulations result in the average power of a chaos modulated symbol being unity [19]. By using the Gaussian symbol s_{n,m_2} in Eq. (7), the transmission symbol sequence $\mathbf{s}_n(u)$ from the nth short bit sequence $\mathbf{b}_n(u)$ for each user is obtained with the following equation. In this modulation process, $N_\mathrm{t}B$ symbols are generated from $N_\mathrm{t}B$ bits, such that the transmission efficiency is 1 bit/symbol/antenna.

$$\mathbf{s}_n(u) = \left\{s_{n,0}, \cdots, s_{n,N_\mathrm{t}B-1}\right\} \tag{9}$$

This symbol sequence is transmitted through N_t MIMO antennas B number of times, and then, N_t symbols are transmitted in each of those time sequences. The MIMO transmission vector at a certain time t $(1 \leq t \leq B)$ is expressed as

$$\mathbf{s}_n(u,t) = \left\{s_{n,1}(t), \cdots, s_{n,N_\mathrm{t}}(t)\right\}^\mathrm{T} \tag{10}$$

where T represents the transpose operation, and each element in Eq. (10) is transmitted through each antenna. Thus, one MIMO transmission block for user u is expressed as

$$\mathbf{s}_{B,n}(u) = \begin{bmatrix} s_{n,1}(1) & \cdots & s_{n,1}(B) \\ \vdots & \ddots & \vdots \\ s_{n,N_\mathrm{t}}(1) & \cdots & s_{n,N_\mathrm{t}}(B) \end{bmatrix} \tag{11}$$

2.1.2 User scheduling and non-orthogonal signal multiplexing

The user allocation and superposition in the power domain at each subchannel in a C-NOMA scheme is described. It is assumed that the total N_c subcarrier allocated to each user is 1 OFDM frame. Note that in a C-NOMA system, one MIMO transmission block for a certain user is composed of B MIMO vectors as can be seen in Eq. (11). Therefore, the user scheduling is conducted per B subcarrier unit as one subchannel, and the number of total subchannels is N_c/B. In this system, OMA or NOMA allocation, with m_s maximum users, is technically selected according to the CSI between the BS and each UE. When the NOMA transmission scheme is selected, users to be superimposed at the jth subchannel are denoted as

$$\mathrm{U}_j = \left\{I_j(1), I_j(2), \cdots, I_j(i)\right\} \tag{12}$$

where $I_j(i)$ $(1 \leq I_j(i) \leq K)$ is the ith user transmitted on the jth subchannel, and the ranges of indexes i and j are $1 \leq i \leq m_\mathrm{s}$ and $1 \leq j \leq N_\mathrm{c}$/B, respectively. The derivation for the user selection of U_j is given in Eq. (17). Next, the

NOMA transmission vector for U$_j$ is generated, and its corresponding vector at *t*th subcarrier in the *j*th subchannel is given as

$$\mathbf{x}_t = \sum_{i=1}^{m_s} \sqrt{p_t\left(I_j(i)\right)}\, \mathbf{s}_j\left(I_j(i), t\right) \tag{13}$$

where (comment #3–5) the vector $\mathbf{s}_j(I_j(i), t)$ is the transmission vector for user $I_j(i)$ and corresponds to the *t*th MIMO transmission vector in the *n*th transmission block $\mathbf{s}_n(u, t)$ of the $I_j(i)$-th user. (Comment #3–5) The scalar $p_t(I_j(i))$ indicates the transmission power for user $I_j(i)$, and the total transmission power of each (comment #3–2) subchannel is expressed as

$$\sum_{t=1}^{B}\sum_{i=1}^{m_s} p_t\left(I_j(i)\right) = B{\cdot}P \quad : \text{constant} \tag{14}$$

The subchannel allocation in C-NOMA is conducted based on the channel capacity between the BS and all the UEs. At the BS, the channel capacity of user $I_j(i)$ at the j th subchannel per 1 Hz is calculated as

$$R_j\left(I_j(i)|U_j\right) = \sum_{t=1}^{B} \log_2\left(1 + \frac{G_{j,t}\left(I_j(i)\right)p_t\left(I_j(i)\right)}{N_{j,t}\left(I_j(i)\right)}\right) \tag{15}$$

where $N_{j,t}(I_j(i))$ is the average power of the thermal noise vector $\mathbf{n}_{j,t}(I_j(i))$ at the receiver $I_j(i)$, and $G_j(I_j(i))$ is the channel power of $I_j(i)$ at the *t*th subcarrier on the *j*th subchannel, which can be written as

$$G_{j,t}\left(I_j(i)\right) = \sum_{v=0}^{N_{\min}} \lambda_{j,t,v}\left(I_j(i)\right) \tag{16}$$

where $N_{\min} = \min(N_t, N_r)$, and N_r is the number of receiver antennas. $\lambda_{j,t,v}(I_j(i))$ is the *v*th eigenvalue of $\mathbf{h}_{j,t}(I_j(i))$, where $\mathbf{h}_{j,t}(I_j(i))$ is the $N_r \times N_t$ – dimensional channel matrix between the BS and user $I_j(i)$ at the *t*th subcarrier on the *j*th subchannel. It is assumed that $\mathbf{h}_{j,t}(I_j(i)$) is absolutely registered at the BS via feedback information. In conventional NOMA schemes with successive interference cancelation (SIC) [6], the channel capacity in Eq. (15) is calculated based on the signal-to-interference-plus-noise ratio (SINR) criterion, and the assumption that the superimposed signal from users within close proximity is treated as interference, and its component eventually added to the denominator of Eq. (15) [19]. (Comment #2–3) Furthermore, when MIMO-NOMA is used, there is an inter-stream interference in addition to the inter-user interference, and the order of SIC becomes important. However, in the proposed scheme, the joint maximum likelihood sequence estimation (MLSE) including the target and superimposed users is performed to obtain better decoding performances, as described in Section 2.1.1. The SNR criterion in Eq. (15) therefore becomes the optimum capacity equation for each user. (Comment #2–3) The proposed scheme based on MIMO-NOMA-SIC will be considered in future studies.

In the NOMA scheme, multiple users having different channel conditions are selected as the non-orthogonal superimposed pair based on Eqs. (15) and (16). In this work, a proportional fair (PF) scheduling algorithm which considers the uniformity among users on a subchannel basis is adopted. Based on [20], and considering an MIMO block length B, the user combination U$_j$ is determined for each subchannel as follows:

$$U_j = \max_{U} Q_j(U)$$

$$Q_j(U) = \sum\nolimits_{u_2 \in U}\left(\frac{R_j(u_2|U, t_2)}{L(u_2, t_2)}\right) \tag{17}$$

where $Q_j(U)$ is the scheduling metric of the candidate user for superimposition U, and the combination of users having the maximum value is determined as the pair U_j in the *j*th subchannel, including OMA and NOMA. This $Q_j(U)$ is the sum of the metrics of allocated users in the combination candidate U, and the total number of combinations of the candidate user set N_U is given as

$$N_U = \binom{K}{1} + \binom{K}{2} + \cdots + \binom{K}{m_s} \tag{18}$$

$R_j(u_2|\, U, t_2)$ in Eq. (17) indicates the channel capacity of user u_2 allocated to *j*th subchannel at time t_2. If a user is unassigned, the value of $R_j(u_2|\, U, t_2)$ becomes 0. $L(u_2, t_2)$ is the average throughput of user u_2 at time t_2,and is defined as

$$L(u_2, t_2) = \left(1 - \frac{1}{t_c}\right)L(u_2, t_2 - 1) + \frac{1}{t_c}\left(\frac{B}{N_c}\sum_{j=1}^{N_c/B} R_j(u_2, t_2 - 1)\right) \tag{19}$$

where t_c is an averaging parameter in the time direction, and is set to 20 in this study. User scheduling based on Eq. (17) produces a high capacity allocation, while considering uniformity among users in the NOMA system.

In the NOMA transmission, since the signals for each user are superimposed in the power domain on each subchannel, it is necessary to carefully allocate the transmission power to each user so as not to significantly deteriorate the throughput of the entire system. One of the methods that can be employed to carry out such allocation is fractional transmit power control (FTPC). In this approach, the transmission power allocated to users on each subcarrier in one subchannel is determined based on the channel gains of the superimposed users as follows:

$$p_t\left(I_j(i)\right) = \frac{P}{\sum_{u_3 \in U_j}\left(G_{j,t}(u_3)/N_{j,t}(u_3)\right)^{-\alpha_{\mathrm{FTPC}}}}\left(\frac{G_{j,t}\left(I_j(i)\right)}{N_{j,t}\left(I_j(i)\right)}\right)^{-\alpha_{\mathrm{FTPC}}} \tag{20}$$

α_{FTPC} $(0.0 \leq \alpha_{\mathrm{FTPC}} \leq 1.0)$ is a parameter for adjusting the allocated power difference, and when α_{FTPC} approaches 1.0, the higher power is allocated to the low-channel gain user. In C-NOMA configuration, this parameter is set to 0.0, and equal power is allocated to each user to obtain the best decoding performance in the joint MLSE. (Comment #3–4) MLSE offers the best decoding performance when the received SNR is maximum and a posteriori probability is maximized. When the number of accommodated users is assumed to be 2, the following relationship is expressed based on the Cauchy–Bunyakovski–Schwarz inequality as

$$\|\mathrm{SNR}_1 + \mathrm{SNR}_2\| \leq \|\mathrm{SNR}_1\| + \|\mathrm{SNR}_2\|, \tag{21}$$

where SNR_1 and SNR_2 are the SNRs of each user, and the left term of (21) indicates the SNR of the received NOMA signal. In (21), the equality phenomenon is obtained when $\|\mathrm{SNR}_1\| = \|\mathrm{SNR}_2\|$, which signifies that equal power is allocated to two users because of downlink transmission. In this case, the SNR of the received NOMA signal is maximized and the performance of MLSE becomes superior to the other options. As a result, simultaneously considering Eq. (14) under the condition, $P = 1.0$ and 2 superimposition, $p_t(I_j(i))$ is set to 0.5 for both users.

2.2 Decoding in receiver of user equipment

Additional file 3: Figure S3 outlines the operational process of a UE receiver. It is assumed that U_j is completely recorded on each UE via any control signals, and the chaos demodulation from the received NOMA signals after subcarrier extraction is considered. User $I_j(i)$ receives the following vector at the tth subcarrier on the jth subchannel:

$$\mathbf{y}_{j,t}\left(I_j(i)\right) = \mathbf{h}_{j,t}\left(I_j(i)\right)\mathbf{x}_t + \mathbf{n}_{j,t}\left(I_j(i)\right) \tag{22}$$

Collecting $\mathbf{y}_{j,\ t}(I_j(i))$ for all t, the chaos demodulation for subchannel j is executed. (Comment #2–3) The demodulation technique using SIC is widely studied for NOMA transmission, and it has been shown in [5] that SIC can be applied to MIMO schemes. However, in this paper, we utilize MLSE for demodulation because of its excellent decoding performance. If OMA is used, the single-user MLSE demodulation [7] is selected. The nth received bit sequence is obtained as

$$\hat{\mathbf{b}}_n = \underset{\mathbf{b}_n}{\mathrm{argmin}} \sum_{t_3=1}^{B} \|\mathbf{y}_n(t_3) - \mathbf{H}_n(t_3)\hat{\mathbf{s}}_n(t_3)\|^2 \tag{23}$$

where $\mathbf{y}_n(t_3)$, $\mathbf{H}_n(t_3)$, and $\hat{\mathbf{s}}_n(t_3)$ are the nth received vector, channel matrix, and estimated transmitted vector at the t_3th subcarrier, respectively, corresponding to the extracted jth subchannel. To generate the same chaos signal used in the transmitter in Eq. (22) at the receiver, the same signal key in Eq. (2) at the transmitter is required. This MLSE in Eq. (22) is the same as C-MIMO decoding [7]. However, Eq. (22) cannot be applied for NOMA decoding because of the superimposed user interference. Therefore, in the NOMA transmission, the joint MLSE while considering other user components is conducted, and the desired bit sequence for user $I_j(i)$ is extracted. The user $I_j(i)$ can obtain the desired bit sequence from jth subchannel as

$$\begin{aligned}\hat{\mathbf{b}}_n = \underset{\mathbf{b}_{j},\ \ \mathbf{b}_{\mathrm{I},j}}{\mathrm{argmin}} \sum_{t=1}^{B} \Big\| \mathbf{y}_{j,t}\left(I_j(i)\right) - \mathbf{h}_{j,t}\left(I_j(i)\right)\Big\{ p_t\left(I_j(i)\right)\hat{\mathbf{s}}_j\left(I_j(i), t\right) \\ + \sum\nolimits_{u_2 \in U_j} p_t(u_2)\hat{\mathbf{s}}_{\mathrm{I},j}(u_2, t)\Big\}\Big\|^2\end{aligned} \tag{24}$$

where $\hat{\mathbf{s}}_j\left(I_j(i), t\right)$ is the candidate of estimated MIMO vector for the target user $I_j(i)$, $\mathbf{b}_{\mathrm{I},\ j}$ and $\hat{\mathbf{s}}_{\mathrm{I},j}(u_2, t)$ are the estimated candidate bit sequence and vector of the superimposed components, respectively. During demodulation, user $I_j(i)$ can also obtain the bit sequence of the superimposed user u_2. However, it is assumed that the superimposed user signals are only utilized in the joint MLSE, and the decoded results $\mathbf{b}_{\mathrm{I},\ j}$ are discarded at $I_j(i)$. Furthermore, to execute Eq. (23), user $I_j(i)$ needs both its key and those of the superimposed users. For example, if two users are superimposed, both must share the signal keys corresponding to the NOMA user set U_j with each other and the BS, otherwise, neither can correctly decode the received signals. Therefore, (comment #3–3) different from the C-MIMO scheme, the proposed C-NOMA configuration requires key exchange among users, which simultaneously triggers a strong physical layer security effect owing to the fact that the number of key signals required for proper demodulation without interference increases. Because the user pair U_j changes on every subchannel in NOMA transmission, each user needs to hold the signal keys of all potential users in the target cell as a group. Thus, the C-NOMA setup is a group encryption scheme. Moreover, the performance obtainable using Eq. (23) is maximized when the posteriori probability of the entire received sequence is also exploited, and in this regard, the allocated transmission power is equally distributed among all users as described in Section 2.1.2.

2.3 Calculation complexity during demodulation at UE

Table 1 lists the calculation complexity of the chaos demodulation per subchannel (=B subcarriers), when a UE receives a NOMA transmitted signal in C-NOMA. The transmission efficiency of the C-NOMA and C-OFDMA schemes described in Section 2.1.1 is the same as BPSK, and those of BPSK-NOMA and BPSK-OFDMA are also tabulated for comparison purpose. Note that in the BPSK-NOMA scheme, it is assumed that the joint maximum likelihood decoding (MLD) for both desired and interfering users is conducted as in Eq. (23) for even comparison to the C-NOMA setup. The contents of the last row in Table 1 highlights an example of the associated complexity during demodulation when $N_t = 2$, $B = 2$ and $m_s = 2$. Because the proposed C-NOMA scheme uses the joint MLSE for chaos block demodulation including superposed users and MIMO detection, the calculation complexity of C-NOMA largely increases compared to other schemes. Thus, when the maximum number of multiplexing users m_s is large, the decoding complexity in C-NOMA significantly increases. Therefore, the reduction of the decoding complexity in the C-NOMA scheme using methods like SIC, in which the interference is sequentially eliminated, should be considered in future studies as m_s increases. Currently, C-NOMA-SIC does not operate well in terms of decoding performance.

3 Numerical results

The transmission performance of the C-NOMA scheme by numerical simulations is evaluated and compared to other schemes. The basic simulation conditions are listed in Table 2. A downlink transmission is assumed, and a regular hexagonal single cell model where $K = 8$ is randomly distributed. The maximum number of multiplexing users m_s is set to 2, and the NOMA transmission with 2-user superimposition or OMA (OFDMA) is appropriately selected. The number of subcarrier in one OFDM frame is $N_c = 256$, and the FFT size is equal to N_c. The MIMO block length is set to 2, and one OFDM frame is divided into every consecutive two subcarriers. The total number of subchannels is 128. 2 × 2 MIMO antennas for the BS and each UE, and the channel is 16-path 1 dB-decay quasi-static Rayleigh fading. The path loss exponent and the standard deviation of the shadowing loss are 3.5 and 7.0 dB, respectively. It is assumed that the CSI of all users is fully registered at the BS and UEs, and all keys are shared with the users in the target cell. The user scheduling is conducted by applying the PF criterion on each subchannel, and no outer channel coding was used.

Table 2 Basic simulation conditions

Proposed downlink chaos NOMA scheme	
Cell layout	Hexagonal single-cell model
No. of antennas	$N_t = N_r = 2$
No. of users K [/cell]	8
Max. user multiplexing m_s	2
Power decay factor α_{FTPC}	0.0 (equal power allocation)
No. of subcarrier N_c	256
FFT size	256
Channel	16 pass 1 dB decayed quasi-static Rayleigh fading + AWGN
Path loss exponent	3.5
Standard deviation of shadowing loss [dB]	7.0
Channel estimation	Ideal
Scheduling algorithm	Proportional fairness
MIMO block length	$B = 2$
Chaos modulation [bit/symbol/antenna]	1
Chaos generation	Bernoulli shift map
No. of chaos processing	Ite = 100
Chaos demodulation	MLSE
Outer channel coding	None

3.1 Transmission performances

To evaluate the basic transmission performance of C-NOMA, the system average bit error rate (BER) and the average system throughput versus the average received SNR per antenna at the cell edge are calculated. Additional file 4: Figure S4a and b show the BER performance and the system throughput, respectively. In the figures, the reference, BPSK-NOMA transmission which has the same efficiency as C-NOMA, and C-OFDMA with physical layer encryption [14], is plotted along with them. The demodulation schemes for BPSK-NOMA and C-OFDMA are the joint MLD which are nearly identical as in Eq. (24) and MLSE in Eq. (23), respectively. In addition, the NOMA power offset $\alpha_{FTPC} = 0.4$ is applied for BPSK-NOMA in order to prevent degradation by zero signal convergence after superposition, and also to exploit the joint MLD effect. According to this weighted power allocation, the capacity equation for user scheduling is changed to maximize the BER and throughput performances in BPSK-NOMA with joint MLD, and is given as follows:

Table 1 Decoding computational complexities

	C-NOMA	C-OFDMA	BPSK-NOMA	BPSK-OFDMA
Decoding computational complexities	$(2^{N_t B})^{m_s}$	$2^{N_t B}$	$2^{N_t m_s} B$	$2^{N_t} B$
	$(2^4)^2 = 2^8$	2^4	$2^4 \times 2 = 2^5$	$2^2 \times 2 = 2^3$

$$R_j\left(I_j(i)|U_j\right) = \sum_{t=1}^{B} \log_2\left(1 + \frac{G_{j,t}\left(I_j(i)\right)p_t\left(I_j(i)\right) + \sum_{i_2\in U_j,\ \frac{G_{j,t}\left(I_j(i)\right)}{N_{j,t}\left(I_j(i)\right)}<\frac{G_{j,t}\left(I_j(i_2)\right)}{N_{j,t}\left(I_j(i_2)\right)}} \sqrt{G_{j,t}\left(I_j(i)\right)p_t(i_2)}}{\sum_{i_2\in U_j,\ \frac{G_{j,t}\left(I_j(i)\right)}{N_{j,t}\left(I_j(i)\right)}<\frac{G_{j,t}\left(I_j(i_2)\right)}{N_{j,t}\left(I_j(i_2)\right)}} \sqrt{G_{j,t}\left(I_j(i)\right)p_t(i_2)} + \sqrt{N_{j,t}\left(I_j(i)\right)}}\right) \tag{25}$$

$$R_j\left(I_j(i)|U_j\right) = \sum_{t=1}^{B} \log_2\left(1 + \frac{\left\{G_{j,t}\left(I_j(i)\right)p_t\left(I_j(i)\right)\right\}^2 + \sum_{i_2\in U_j,\ \frac{G_{j,t}\left(I_j(i)\right)}{N_{j,t}\left(I_j(i)\right)}<\frac{G_{j,t}\left(I_j(i_2)\right)}{N_{j,t}\left(I_j(i_2)\right)}} G_{j,t}\left(I_j(i)\right)p_t(i_2)}{\sum_{i_2\in U_j,\ \frac{G_{j,t}\left(I_j(i)\right)}{N_{j,t}\left(I_j(i)\right)}<\frac{G_{j,t}\left(I_j(i_2)\right)}{N_{j,t}\left(I_j(i_2)\right)}} \left\{G_{j,t}\left(I_j(i)\right)p_t(i_2)\right\}^2 + N_{j,t}\left(I_j(i)\right)}\right) \tag{26}$$

where Eqs. (25) and (26) maximize the BER performance and throughput, respectively. These equations are based on the SIC scheme of [13] and are modified using a trial-and-error approach to improve the performances. (Comment 2–4) It is important to verify the performance of the proposed C-NOMA with the theoretical results. Although the theoretical analysis of C-MIMO has been studied in [7], the derivation of theoretical C-NOMA-MLSE and BPSK-NOMA-MLD performances in cell model without any user distribution limitation is quite complicated. But, in this study, the upper and lower performance limits were demonstrated using a concentric user distribution with inner and outer rings in the simulation.

As a result, it is shown in Additional file 4: Figure S4a that the proposed C-NOMA has a large coding gain for the unencrypted BPSK-NOMA transmission. This is because of the channel coding effect generated by the C-MIMO. Compared to the BPSK-NOMA method, its gain is about 5 dB at an average BER of 10^{-5}. (Comment 2–4) When comparing the performance with the upper and lower limits, it was found that the numerical results were within both bounds and the lower limit of C-NOMA is nearly free of any observable error. Note that the upper and lower limits of BPSK-NOMA overlap each other due to the mismatch setting of the power offset α_{FTPC} for the concentric user distribution. Also, the BER of a third party without the valid keys (initial values) attempting to demodulate the transmitted signals, is plotted as "C-NOMA, unsync." It was observed that the BER becomes 0.5 regardless of the average SNR received, and thus the correct information is inaccessible. Therefore, the physical layer security effect is proven with the C-NOMA scheme against a third party without the correct keys. Similarly, in Additional file 4: Figure S4b, the performance of the C-NOMA setup is superior to the unencrypted BPSK-NOMA, reaching the maximum throughput when the average SNR is about 15 dB. (Comment 2–4) This advantage of C-NOMA is also confirmed in comparing the upper and lower limits in the figure. Moreover, in comparison with the C-OFDMA method, which is the same encrypted transmission scheme as the proposed C-NOMA technique—although the BER is inferior because the allocated power per user decreases in the case of C-NOMA—the number of accommodated users increases because of the NOMA architecture, and accordingly, the system capacity can be increased while maintaining the physical layer security.

Consequently, based on the above results and details given in Section 2.2.3, the proposed C-NOMA scheme improves the BER performance for unencrypted scheme with the same transmission efficiency. A similar performance impact on the throughput was observed for C-OFDMA transmission, which is an encrypted transmission scheme, but the compromise is an increase in the calculation complexity during the decoding phase. By exploiting the chaos-based NOMA, both higher capacity and physical layer security are achieved.

3.2 Configuration of signal keys and chaos iteration number among users

We investigated the influence of the configuration of signal keys and chaos iteration number among users for the BER performance in the C-NOMA scheme to clarify the restrictions of the signal keys. As presented in Table 3, four patterns of key allocation are assumed, and the performances are calculated in each case. Pattern I has the same configurations as in Additional file 4: Figure S4, and for pattern IV, the signal keys and iteration number are identical for all users. Pattern II has a different iteration number only, and pattern III has a different signal key and iteration number for each user.

As shown in the graph of Additional file 5: Figure S5, a significant degradation appears only in pattern IV and there is no noticeable difference in the BER performance

Table 3 Allocation pattern of signal key and chaos processing number

Allocation pattern		
	Signal keys	No. of chaos processing
I	$c_{00,\,1} \neq c_{00,\,2} \neq \cdots \neq c_{00,\,K}$	$\mathrm{Ite}_1 = \mathrm{Ite}_2 = \cdots = \mathrm{Ite}_K = \mathrm{Ite}$
II	$c_{00,\,1} = c_{00,\,2} = \cdots = c_{00,\,K}$	$\mathrm{Ite}_h = \mathrm{Ite} + 3(h-1)$, $(h = 1, \cdots, K)$
III	$c_{00,\,1} \neq c_{00,\,2} \neq \cdots \neq c_{00,\,K}$	$\mathrm{Ite}_h = \mathrm{Ite} + 3(h-1)$, $(h = 1, \cdots, K)$
IV	$c_{00,\,1} = c_{00,\,2} = \cdots = c_{00,\,K}$	$\mathrm{Ite}_1 = \mathrm{Ite}_2 = \cdots = \mathrm{Ite}_K = \mathrm{Ite}$

for the other patterns. The behavior of chaos signal is determined by two elements of the signal key and chaos iteration number, and the same chaos signal is generated only when the same configuration for both parameters is used. In pattern IV, the correlation between the signals to be superimposed becomes high, such that the BER performance is diminished due to the indistinguishable nature of the target and superimposed signals, and also the target signal being irretrievable under equal power allocation. However, from other results, it is clear that the proposed C-NOMA performs adequately only if the signal key or chaos iteration number is different among users. On the other hand, in pattern III, because more varied configurations are used compared to patterns I and II, the security strength in this scenario is enhanced.

3.3 Security evaluation against proximity of initial keys at eavesdroppers

The security capability of the C-NOMA scheme is analyzed in this section. It is assumed that the eavesdropper exists in the cell and tries to replicate the received signals. In this analysis, we use the equivalent channel capacity C_{E} as the evaluation index calculated from the BER performance of the eavesdropper [21], which is given as

$$C_{\mathrm{E}} = N_{\mathrm{rE}}\left[1 + P_{\mathrm{rE}}\log_2 P_{\mathrm{rE}} + (1 - P_{\mathrm{rE}})\log_2(1 - P_{\mathrm{rE}})\right], \tag{27}$$

where N_{rE} is the minimum number of transmission and receiving antennas between the BS and the eavesdropper, and P_{rE} is the BER of the eavesdropper. The larger the value of C_{E}, the higher the chances of the eavesdropper obtaining the transmission data in the system. N_{rE} and the number of legitimate users is assumed to be 2, while the maximum value of C_{E} is 2 bit/symbol. It is also assumed that the eavesdropper targets the following signals: [a] OFDMA transmission signal, [b] NOMA transmission signal for a user near the BS, [c] NOMA transmission signal for a user far from the BS. In the NOMA transmission, $m_{\mathrm{s}} = 2$, and thus, two signal keys are needed to correctly demodulate the received superimposed signal as described in Section 2.2.2. The keys of the target and superimposed users are designated as the main key and sub key, respectively. Following this stage, the security capability of the different transmission schemes is evaluated. To carry out this analysis, two scenarios were established as [I] a case where the eavesdropper obtains the main key via any means and attempts to estimate the sub key, and [II] a case where the eavesdropper obtains the sub key and proceeds to estimate the main key.

Additional file 6: Figure S6 shows the equivalent channel capacity of an eavesdropper versus the difference of estimated key from the correct key based on the conditions tabulated in Table 2. The average SNR at the cell edge per receiving antennas at the eavesdropper is assumed to be either 10 or 20 dB. The horizontal axis in Additional file 6: Figure S6 represents the estimation accuracy of the signal key, and the larger this value is, the closer the eavesdropper is to obtaining the key of a legitimate user. The results of Additional file 6: Figure S6 also reveal that regardless of the scenario, at $x = 16$, if the accuracy of the estimated key is close to 10^{-16} or more of the correct key, the eavesdropper can obtain the entire available information in the system. Otherwise, the obtained channel capacity is low, and in particular, scenario [II], where the capacity is almost zero regardless of OFDMA or NOMA transmission type. Thus, in the proposed scheme, the integrity of the system can be maintained if the estimation on the main key by the eavesdropper for a target user is insufficient. According to the results of scenario [I] in Additional file 6: Figure S6a, even in the case that the eavesdropper eventually obtains the main key, the desired signal in the C-NOMA transmission system is embedded deeply in the interference, and the leakage probability is low and below an accuracy of 10^{-16} of the sub key. However, for C-OFDMA signals, the eavesdropper has access to the maximum channel capacity because C-OFDMA signals can be demodulated only with the main key, as described in Section 2.2.2. In addition to capacity enhancement, the proposed C-NOMA transmission scheme has an advantage of strong physical layer security because the eavesdropper would require more than two keys for accurate decoding.

4 Conclusions

A downlink chaos non-orthogonal multiple access scheme (C-NOMA), which provided high capacity allocation and physical layer security by applying the principle of C-MIMO scheme was presented in this paper. Simulations results show that the proposed C-NOMA configuration offered not only physical layer security, but also improved BER performance, compared to the conventional power domain NOMA. Furthermore, in comparison with the conventional C-OFDMA method, C-NOMA was demonstrated as a system with enhanced system capacity function. The security capability against an eavesdropper using the equivalent channel capacity was evaluated and showed that a strong security system could be established via multiple user transmission of C-NOMA. Conversely, the primary drawback of this technique is the considerable increase in the decoding complexity for the number of superimposed users.

In future studies, we shall consider a calculation reduction method for UE decoding in the C-NOMA scheme, and an improvement method for the system performance using an outer channel code concatenation and log-likelihood (LLR) calculation from chaos signals.

5 Methods/experimental

The aim of this study is to propose a new wireless communication method. To show the new contributions and their effectiveness, we conducted the numerical simulations, in which C programs were constructed and GNU Compiler Collection was used. No experiment involving human participants or animals was conducted.

6 Additional files

Additional file 1: Figure S1. Illustration of a downlink NOMA transmission scheme. (BMP 4333 kb)

Additional file 2: Figure S2. System model of the base station transmitter. (BMP 3448 kb)

Additional file 3: Figure S3. System model of a UE receiver. (BMP 2940 kb)

Additional file 4: Figure S4. Comparison of transmission performances for average SNR received per antenna. (a) Average bit error rate. (b) Average system throughput. (BMP 4074 kb)

Additional file 5: Figure S5. BER performances for different user configurations. (BMP 4299 kb)

Additional file 6: Figure S6. Equivalent channel capacity of the eavesdropper. (a) scenario [I]. (b) Scenario [II]. (BMP 4621 kb)

Abbreviations

LTE: Long-term evolution - Mobile phone standards that were formulated in March 2009 under the third generation partnership project (3GPP) Release 8 at 3GPP, a standards body; ICT: Information and communication technology - Generic name of technology, industry, equipment, service, etc. related to information processing and communication; OFDM: Orthogonal frequency-division multiplexing - One of digital signal modulation methods widely adopted in wireless local area network (LAN) and LTE and so on. By placing each subcarrier orthogonally and densely, this method can effectively utilize the limited frequency band and reduce the influence of multipath in this method; OFDMA: Orthogonal frequency division multiple access - Wireless communication scheme based on OFDM accommodating multiple users. In this scheme, a technique is adopted in which multiple users share subcarriers, and subcarriers with the highest transmission efficiency are allocated to each user; NOMA: Non-orthogonal multiple access - Multiple access method being studied based on the standardization of 5G. By superimposing multiple users non-orthogonally to one subcarrier, large capacity communication compared to OFDMA is realized; MIMO: Multiple-input multiple-output - A wireless communication technology which has multiple antennas on the transmitter and the receiver, and transmits data via these devices; C-MIMO: Chaos multiple-input multiple-output - Wireless communication system with physical layer security based on MIMO system which has been proposed in the current study. This scheme is a common-key encryption scheme, and as a result, transmission can be correctly performed only when the same key is shared with the transmitter and receiver, and it also has confidentiality to a third party; C-NOMA: Chaos non-orthogonal multiple access - A multiple access scheme with physical layer security which has been proposed in this paper. In this method, the chaos modulation signal used in chaos MIMO is superimposed in the power domain and transmitted from the transmitter; C-OFDMA: Chaos orthogonal frequency-division multiple access - A multiple access scheme proposed in this study, in which chaos modulated signals are transmitted based on the OFDMA scheme; BS: Base station - Equipment including antennas and devices for directly communicating with wireless communication terminals; UE: User equipment - A wireless communication terminal such as a cellular phone that communicates with a base station; OMA: Orthogonal multiple access - Unlike NOMA, it is a designation when one user is assigned and communicating on one orthogonal subcarrier; CSI: Channel state information - State of propagation path between the base station and user terminal; FFT: Fast Fourier transform - Signal processing technique used for the modulation and demodulation processing of OFDM, in addition to frequency analysis of signals such as images/sounds; IFFT: Inverse fast Fourier transform - Similar to FFT, signal processing technique used for the modulation and demodulation processing of OFDM, in addition to frequency analysis of signals such as images/sounds. IFFT is a signal processing operation opposite to FFT; GI: Guard interval - The interval inserted between the symbol to be transmitted and the symbol. Thus, the influence of interference between symbols can be reduced, and it is used in OFDM and OFMDA or the like; SINR: Signal-to-interference noise ratio - A ratio of power other than the desired signal such as power of the desired signal and noise and interference from other cells; MLSE: Maximum likelihood sequence estimation - Signal detection method based on maximum a posteriori probability. The calculation complexity becomes huge in exchange for high detection accuracy; PF: Proportional fairness - One of scheduling methods considering fairness among accommodated users, which is used when allocating subcarriers to users in the multiple access method; FTPC: Fractional transmit power control - A method of power allocation among users in NOMA transmission; MLD: Maximum likelihood detection - As with MLSE, signal detection method based on maximum a posteriori probability used in the MIMO scheme

Acknowledgements

This work was supported by JSPS KAKENHI, Grant Number JP18K04136.

Funding

JSPS KAKENHI, Grant Number JP18K04136.

Authors' contributions

NH (first author) and EO (second author) made contributions to the project conceptualization and design, and analysis and interpretation of data, and were involved in drafting and revising the manuscript. All authors read and approved the final manuscript.

Authors' information

Naoto Horiike received the B.E. degree in Electrical Engineering from the Nagoya Institute of Technology in 2016. He is currently studying for his in the Master's degree at the same institution. His research interests include wireless communication and encryption techniques.
Eiji Okamoto received the B.E. degree and the M.S. degree in Electrical Engineering from Kyoto University, Japan in 1993 and 1995, respectively. In 1995, he joined the Communications Research Laboratory (CRL), Japan. He also received the Ph.D. degree from the same university. Currently, he is an Associate Professor at Nagoya Institute of Technology. His current interests include coded-modulation, satellite communication, and mobile communication systems. He is a member of IEICE and IEEE.
Tetsuya Yamamoto received the B.E. degree in Electrical, Information and Physics Engineering in 2008 and M.S. and Dr. Eng. degrees in communications engineering from Tohoku University, Sendai, Japan, in 2010 and 2012, respectively. From April 2010 to March 2013, he was a Japan Society for the Promotion of Science (JSPS) research fellow. Since April 2013, he has been with Panasonic Corporation. He was a recipient of the 2008 IEICE RCS (Radio Communication Systems) Active Research Award and the Ericsson Best Student Award in 2012.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]Graduate School of Engineering, Nagoya Institute of Technology, Nagoya, Aichi, Japan. [2]Core Element Technology Development Center, Panasonic Corporation, Yokohama, Kanagawa, Japan.

Received: 27 November 2017 Accepted: 30 May 2018
Published online: 17 August 2018

References

1. 3rd Generation Partnership Project (3GPP), RWS-120010, NTT DOCOMO, Requirements, Candidate Solutions & Technology Roadmap for LTE Rel-12 Onward, 2012.
2. 3rd Generation Partnership Project (3GPP) TR38.912 (14.1.0), Study on new radio access technology (release 14), 2017.
3. 3rd Generation Partnership Project (3GPP) TR38.913 (14.3.0), Study on scenarios and requirements for next generation access technologies (release 14), 2017.
4. 3rd Generation Partnership Project (3GPP) TS 36.211 (V10.7.0), Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation, 2013.
5. (comment #2-1) K. Higuchi and A. Benjebbour, Non-orthogonal multiple access (NOMA) with successive interference cancellation for future radio access. IEICE Trans. Commun **E98-B**(3), 403–414 (2015)
6. Y Saito, Y Kishiyama, A Benjebbour, T Nakamura, L Anxin, K Higuchi, Non-orthogonal multiple access (NOMA) for cellular future radio access Proc. IEEE **VTC2013Spring**, 1–5 (2013)
7. E Okamoto, A chaos MIMO transmission scheme for channel coding and physical-layer security. IEICE Trans. Commun. **E95-B**(4), 1384–1392 (2012)
8. N Horiike, H Kitagawa, E Okamoto, and T. Yamamoto, Chaos MIMO-based downlink non-orthogonal multiple access scheme with physical layer security Proc. the 15th IEEE Annual Consumer Communications & Networking Conference (CCNC 2018), 1–7, 2018.
9. Y Li, M Jiang, Q Zhang, Q Li, J Qin, Secure beamforming in downlink MISO nonorthogonal multiple access systems. IEEE Trans. Veh. Technol. **66**(8), 7563–7567 (2017) (Comments #1-1, #1-4, #2-2, #3-6)
10. M Jiang, Y Li, Q Zhang, Q Li, J Qin, Secure beamforming in downlink MIMO nonorthogonal multiple access networks. IEEE Signal Process. Lett. **24**(12), 1852–1856 (2017)
11. Y Zhang, H-M Wang, Q Yang, et al., Secrecy sum rate maximization in non-orthogonal multiple access. IEEE Commun. Lett. **20**(5), 930–933 (2016)
12. M Tian, Q Zhang, S Zhao, Q Li, J Qin, Secrecy sum rate optimization for downlink MIMO nonorthogonal multiple access systems. IEEE Signal Processing Letters **24**(8), 1113–1117 (2017)
13. Y Liu, Z Qin, M Elkashlan, Y Gao, L Hanzo, Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. IEEE Transactions on Wireless Communications **16**(3), 1656–1672 (2017)
14. Z Ding, Z Zhao, M Peng, HV Poor, On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming. IEEE Transactions on Communications **65**(7), 3151–3163 (2017)
15. E Okamoto, Y Inaba, A Tanaka, Chaos-MIMO-OFDMA scheme achieving secure multiple access at physical-layer. Proc. IEEE, APWCS2013 , 26-30 (2013)
16. G Alvarez, S Li, Breaking an encryption scheme based on chaotic baker map. Phys. Lett. A **352**, 78–82 (2006)
17. G Alvarez, JM Amigo, D Arroyo, S Li, *Lessons learnt from the cryptanalysis of chaos-based ciphers, in L. Kocarev, S. Lian (Eds.), Chaos based cryptography theory algorithms and applications, Springer-Verlag* (2011), pp. 257–295
18. GRP Box, ME Muller, A note on the generation of random normal deviates. Annals Math. Stat **29**, 610–611 (1958)
19. E Okamoto, N Horiike, Performance improvement of chaos MIMO scheme using advanced stochastic characteristics. IEICE Communications Express **5**(10), 371–377 (2016)
20. A Benjebbour, L Anxin, Y Saito, Y Kishiyama, A Harada, T Nakamura, System-level performance of downlink NOMA for future LTE enhancements. Proc. IEEE Globecom, pp., 66–70 (2013)
21. F Oggier, B Hassibi, The secrecy capacity of the MIMO wiretap channel. Proc. Int'l Sym.on Information Theory (ISIT), 524–528 (2008)