Secrecy Sum Rate for Two-Way Untrusted Relay in SCMA Networks

Yiteng Huang[1], Shuai Han[1(✉)], Shizeng Guo[1], Ming Li[2], and Zhiqiang Li[1]

[1] Communication Research Center, Harbin Institute of Technology, Harbin, China
hanshuai@hit.edu.cn
[2] China Academy of Space Technology, Beijing, China

Abstract. Sparse code multiple access (SCMA) is a novel non-orthogonal multiple access technology that combines the concepts of CDMA and OFDMA. The advantages of SCMA include high capacity, low time delay and high transfer rate. The information security is also very important in 5G network. Relay is essential to be used for long distance cooperative transmission. In this paper, we consider a two-way relay system that each user pair can only communicate through an untrusted intermediate relay. We regard the intermediate relay as an eavesdropper and the confidential information must be kept secret to it. In order to maximize the sum security capacity, a subcarrier assignment algorithm based on matching theory is proposed in this paper. Finally, the theoretical analysis is verified by simulation. Simulation results show that security performance is improved significantly.

Keywords: Amplify-and-forward · Two-way communication · Untrusted relay · Sparse code multiple access

1 Introduction

In future 5G networks, the data flow rate of the system will be greatly improved and will occupy an increased range of bandwidth compared with 4G networks [1]. Sparse code multiple access (SCMA) is a multidimensional codebook-based technique to increase connectivity and multiuser capacity. SCMA combines the concepts of CDMA and OFDMA [2,3] to achieve non-orthogonal multiple access in the frequency domain. Information theoretic security was proposed by Shannon [4]. Wyner, in [2], pointed out that the eavesdropper only has a noisy copy of the signal transmitted from the source, and building a useful secure communication system per Shannons notion is possible [5,6].

Recent progress in physical layer security area has been extended. Examples include using multiple antennas to steer the transmitted signal away from an eavesdropper [7] or taking advantage of variations in channel state to provide secrecy [8]. According to the information theoretic security, if the wiretap

This work is supported by the National Natural Science Foundation of China (No. 41861134010 and No. 61831002).

X. B. Zhai et al. (Eds.): MLICOM 2019, LNICST 294, pp. 72–83, 2019.
https://doi.org/10.1007/978-3-030-32388-2_7

channel is less noisy than the main channel the secrecy capacity will be zero. Cooperative relaying is utilized to overcome secrecy capacity limitation respectively in [9]. Decode-and-Forward (DF)- and Amplify-and-Forward (AF)-based cooperative relaying protocols are proposed to improve physical layer security. In [10], cooperative jamming is regarded as a promising approach to improve the secrecy capacity by confusing the eavesdropper with cooperative interference. Different cooperative jamming schemes were researched for different communication scenarios in related research work.

The focus of this paper differs from all above models, which is on a class of relay networks where the source and the destination have no direct link and thus can only communicate utilizing an intermediate relay node. It is a communication network whose nodes have different levels of security clearance. In SCMA system, it is inefficiency and costly for two long physical distance communication node to communicate directly without relaying. Thus, in this case, it will uses relay nodes to participate in cooperative communication. In this model, different nodes in the communication network has different levels of security clearance. Examples like this exist in real life. In a government intelligence network or the network of a financial institution, not every node in the network is supposed to have the same level of access to information, despite operating with agreed protocols and serving as relay nodes in the network [11]. The relay node are vulnerable to eavesdropping because of its low level of security clearance. Thus, the relay node is considered to be untrusted. Untrusted relay channels were first studied in [12] and [13], where the intermediate relay acts as both an eavesdropper and a helper.

In this paper, we consider a two-way relay system that each user pair can only communicate through an untrusted intermediate relay. This does not mean that the relay node is malicious. On the contrary, it may be part of the network. We will assume that it is willing to faithfully implement the relay scheme. However, the relay only has low security clearance in the network, so we can't trust the confidential messages that it is relaying [11]. It assumes that the confidential messages are used to identify source nodes for authentication [12]. In order not to be attacked illegally by eavesdroppers, the message should never be leaked to relay nodes. In this case it supposes that there is a eavesdropper on the relay node when designing the relay system. In [14], a relay channel is considered, in which the relay helps to transmit messages from the sender to the receiver. Relays are not only regarded as senders to assist the message transmission, but also as eavesdroppers to obtain some information about the transmission message [15]. The sender wants to send two different types of messages. One is called the public message, which is sent to the receiver and relay. The other is called the private message, which is only sent to the receiver and keep confidential to the relay. Even if there are no external eavesdroppers in the system, security is still a problem. That's because although relays help to forward information to destination, designers still hope the source signal itself keep secret from the relay [14].

The main contributions of this work are as follows:

- This paper studies the physical layer security in relay cooperative SCMA multiple access communication system. The physical layer security model of two-way relay cooperative SCMA network is also established in this paper.
- The untrusted relay works on the amplify-and-forward mode. This paper formulates the subcarrier allocation as a non-convex optimization problem to maximize the total security capacity.
- This paper proposes a subcarrier allocation algorithm based on two-side matching game to enhance the security performance without compromising the communication quality of the system. This paper formulates the subcarrier allocation as a non-convex optimization problem to maximize the total security capacity.

The remainder of this paper is organized as follows. Section 2 presents the two-way relay cooperative SCMA network model, the basic principles of SCMA and physical layer security. The proposed subcarrier allocation algorithm based on user-subchannel swap-matching is introduced in Sect. 3. Next, the security performance of the proposed two-way relay system is verified through simulations presented in Sect. 4, and the numerical results are discussed in this section. Finally, the conclusions are described in Sect. 5.

2 System Model

2.1 SCMA Link-Level Model

The structure of the SCMA transmitter is shown in Fig. 1. The data streams from multiple users are first processed by an FEC encoder module; subsequently, the encoded data are interleaved to prevent burst errors. The processed data streams are sent to an SCMA encoder and directly mapped to several orthogonal subcarriers according to predesigned codebooks. Finally, the full data stream outputs from the SCMA encoder are transmitted through the channel.

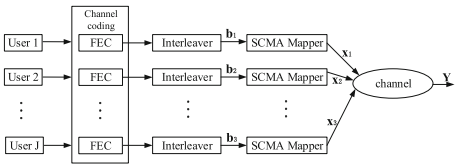

Fig. 1. SCMA transmitter structure

The transmitted signal is superimposed onto the data of other users carried by the same subcarrier, which introduces noise in the transmission process. Then,

the transmitted signal is sent to the receiver. At the receiver, the received symbol can be expressed as

$$\mathbf{y} = \sum_{j=1}^{J} \mathrm{diag}(\mathbf{h}_j)\mathbf{x}_j + \mathbf{n}, \tag{1}$$

where $\mathbf{h}_j = (h_{1j}, h_{2j}, ..., h_{Kj})^T$ is the channel transmission vector of user j, indicating signal attenuation during transmission; $\mathbf{x}_j = (x_{1j}, x_{2j}, ..., x_{Kj})^T$ is the SCMA codeword of user j; and $\mathbf{n}$ is Gaussian white noise in the complex domain.

The SCMA receiver structure is shown in Fig. 2. The SCMA decoder detects the user data streams that have interference by channel noise and other user data streams according to known codebook and subcarrier allocation information. Subsequently, the convolution code is decoded, and the data bits are restored with hard decisions.

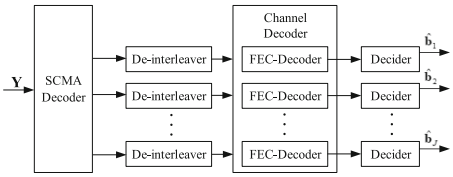

Fig. 2. SCMA receiver structure

2.2 Two-Way Untrusted Relay in SCMA System

A two-way untrusted relay SCMA system is shown in Fig. 3. We consider a two-way relay scenario, which exists many user pair in the system. Each user pair consists two sources, which communicate with each other with the help of an untrusted intermediate relay. Each source is equipped with a single omnidirectional antenna and operates in a half-duplex manner. The intermediate relay works in Amplify-and-Forward (AF) mode in this study.

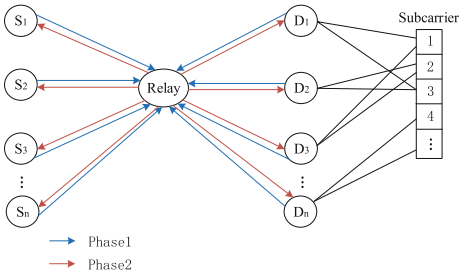

Fig. 3. System model of two-way untrusted relaying

Suppose that there is an untrusted intermediate relay and N user pairs in an SCMA cell. Denote the set of indices $\{1, 2, \cdots, N\}$ by $\mathcal{N}$. Let S_i and $D_i, i = 1, 2, ..., N$ denote the two sources in the same user pair. We denote the user pair as U_i. The intermediate relay divides the available bandwidth of the system into a set of subcarriers, denoted by $\mathcal{K}_{\mathcal{SC}} = \{1, 2, \cdots, K\}$. The signals transmitted from the N user pairs are multiplexed to K orthogonal subcarriers. Then, the communication process can be divided into two stages. In the first stage, all the source nodes in user pairs send their message to the intermediate relay. The user signals are nonorthogonally superimposed on the subcarriers based on multiple access using SCMA. The signal received by malicious relay consists of the superposition of the signals sent by all the source nodes in the system. In the second stage, the intermediate relay amplifies the superposition of received signal and broadcasts it to all the source nodes. There is only one intermediate relay in the system model and no direct link between the two sources of any user pair. Thus, the signal can only be transmitted through the malicious relay to the destination node. We consider a block fading channel, for which the channel remains constant within a certain time-slot, but varies independently from one to another. For subcarrier SC_k, the channel transfer function between source node S_m and intermediate relay is denoted by $h_{k,m} = g_{k,m}/(d_m)^a$, where d_m means the distance between relay and source node S_m, $g_{k,m}$ is the Rayleigh fading channel gain between source node S_m and relay and a is the path loss coefficient. At the relay node, the attenuation signals of different users after channel transmission are superimposed onto each other. Then, the received symbol on the subcarrier SC_k can be expressed as

$$y_{r,i,k} = n_{r,k} + \sqrt{p_{k,s_i}} s_{i,k} h_{k,s_i} + \sqrt{p_{k,d_i}} d_{i,k} h_{k,d_i} + I_{i,k} \tag{2}$$

$$I_{i,k} = \sum_{S_n \in \{S \setminus S_i\}} \left(\sqrt{p_{k,s_n}} s_{n,k} h_{k,s_n} + \sqrt{p_{k,d_n}} d_{n,k} h_{k,d_n} \right), \tag{3}$$

where $n_{r,k}$ denotes the thermal noise at the relay node, $I_{i,k}$ denotes the interference caused by other user signals multiplexing the same subcarrier with the selected user.

Then, the untrusted intermediate relay has the signal-to-noise ratios on the subcarrier SC_k with respect to signals transmitted from user S_i and D_i are as follows

$$\gamma_{s_i}^r = \frac{p_{k,s_i} |h_{k,s_i}|^2}{\delta^2 + p_{k,d_i} {h_{k,d_i}}^2 + \sum\limits_{S_n \in \{S \setminus S_i\}} \left(p_{k,s_n} s_{n,k} |h_{k,s_n}|^2 + p_{k,d_n} d_{n,k} |h_{k,d_i}|^2 \right)} \tag{4}$$

$$\gamma_{d_i}^r = \frac{p_{k,d_i} |h_{k,d_i}|^2}{\delta^2 + p_{k,s_i} |h_{k,s_i}|^2 + \sum\limits_{S_n \in \{S \setminus S_i\}} \left(p_{k,s_n} s_{n,k} |h_{k,s_n}|^2 + p_{k,d_n} d_{n,k} |h_{k,d_i}|^2 \right)} \tag{5}$$

The relay works in AF mode and broadcasts amplified signals to each user node in the downlink. The corresponding signal received by S_i at subcarrier SC_k

can be written as

$$\begin{aligned} y_{s_i,k} &= h_{k,s_i} G_{R,k} y_{r,i,k} + n_{s_i} \\ &= h_{k,s_i} G_{R,k} \left(n_{r,k} + \sqrt{p_{k,s_i}} s_{i,k} h_{k,s_i} + \sqrt{p_{k,d_i}} d_{i,k} h_{k,d_i} + I_{i,k} \right) + n_{s_i} \end{aligned} \tag{6}$$

Similarly, the signal received by D_i at subcarrier SC_k can be written as

$$\begin{aligned} y_{d_i,k} &= h_{k,d_i} G_{R,k} y_{r,i,k} + n_{d_i} \\ &= h_{k,d_i} G_{R,k} \left(n_{r,k} + \sqrt{p_{k,s_i}} s_{i,k} h_{k,d_i} + \sqrt{p_{k,d_i}} d_{i,k} h_{k,d_i} + I_{i,k} \right) + n_{d_i} \end{aligned} \tag{7}$$

As for node S_i, the security capacity at subcarrier SC_k can be expressed as

$$\begin{aligned} C_{k,s_i}^S &= \left(C_{k,s_i} - C_{k,s_i}^r \right)^+ \\ &= \frac{1}{2} \log_2 \left(1 + \frac{{G_{R,k}}^2 {h_{k,d_i}}^2 {h_{k,s_i}}^2 p_{k,s_i}}{\left(1 + {h_{k,d_i}}^2\right) \delta^2 + {h_{k,d_i}}^2 {G_{R,k}}^2 [\sum\limits_{S_n \in \{S \setminus S_i\}} \left(p_{k,s_n} |h_{k,s_n}|^2 + p_{k,d_n} |h_{k,d_n}|^2 \right)]} \right) \\ &\quad - \frac{1}{2} \log_2 \left(1 + \frac{p_{k,s_i} \left| h_{k,s_i} \right|^2}{\delta^2 + p_{k,d_i} {h_{k,d_i}}^2 + \sum\limits_{S_n \in \{S \setminus S_i\}} \left(p_{k,s_n} s_{n,k} |h_{k,s_n}|^2 + p_{k,d_n} d_{n,k} \left| h_{k,d_i} \right|^2 \right)} \right) \end{aligned} \tag{8}$$

Similarly, the security capacity that D_i obtains at subcarrier SC_k can be expressed as

$$\begin{aligned} C_{k,d_i}^S &= \left(C_{k,d_i} - C_{k,d_i}^r \right)^+ \\ &= \frac{1}{2} \log_2 \left(1 + \frac{{G_{R,k}}^2 {h_{k,d_i}}^2 {h_{k,s_i}}^2 p_{k,d_i}}{\left(1 + {h_{k,s_i}}^2\right) \delta^2 + {h_{k,s_i}}^2 {G_{R,k}}^2 [\sum\limits_{S_n \in \{S \setminus S_i\}} \left(p_{k,s_n} |h_{k,s_n}|^2 + p_{k,d_n} |h_{k,d_n}|^2 \right)]} \right) \\ &\quad - \frac{1}{2} \log_2 \left(1 + \frac{p_{k,d_i} \left| h_{k,d_i} \right|^2}{\delta^2 + p_{k,s_i} \left| h_{k,s_i} \right|^2 + \sum\limits_{S_n \in \{S \setminus S_i\}} \left(p_{k,s_n} s_{n,k} |h_{k,s_n}|^2 + p_{k,d_n} d_{n,k} \left| h_{k,d_i} \right|^2 \right)} \right) \end{aligned} \tag{9}$$

Then the system sum security capacity can be expressed as:

$$C^S = \sum_{k=1}^{K} \left(C_{k,s_i}^S + C_{k,d_i}^S \right) \tag{10}$$

3 Secrecy Rate of Two-Way Relay Channel in SCMA System

In order to improve the secrecy performance of relay system, we should design a resource allocation scheme to make more system users get positive security capacity. In the relay system, power amplification and subcarrier allocations are performed by intermediate relay. As for subcarrier allocations, it can be formulated as a many-to-many two-sided matching problem, which can be solved by utilizing the matching theory [16]. The subcarrier allocations scheme will be introduced in this section.

3.1 Subcarrier Allocation Based on Two-Sided Matching Game

We formulate the optimization subcarrier allocation problem into a two-sided matching problem. Then, an optimized subcarrier allocation algorithm is proposed in this section to improve system security performance.

To describe the subcarrier allocation problem, this paper introduces a binary $N \times K$ user pair and subcarrier mapping matrix $F = [f_1, f_2, \cdots, f_N]$. If the subcarrier SC_k is occupied by the mth user pair, $f_{m,k} = 1$, otherwise $f_{m,k} = 0$. Assuming that there are N user pairs and K subcarriers in the system. To evaluate the total security capacity of all users, and then the optimization problem is formulated as:

$$\begin{aligned}
\underset{\mathbf{F}}{\text{maximize}} \quad & \sum_{k=1}^{K}\sum_{n=1}^{N} R_{k,n}\left(p, G\right) f_{k,n}, \\
\text{subject to} \quad & \sum_{n \in N_{user}} f_{k,n} \leq d_f, \forall k \in K_{sc}, \\
& \sum_{k \in K_{sc}} f_{k,n} \leq d_v, \forall n \in N_{user}, \\
& f_{k,n} \in \{0,1\}, \forall k \in K_{sc}, \forall n \in N_{user}, \\
& \sum_{k \in K_{sc}} p_{k,n} \leq P_s, \forall n \in N_{user}, \\
& p_{k,n} \geq 0, \forall k \in K_{sc}, \forall n \in N_{user},
\end{aligned} \tag{11}$$

One subcarrier can be allocated to at most d_f users and one user can access to the system through at most d_v subcarriers. It is a non-convex optimization problem. Thus the complexity of finding the optimal solutions is prohibitive. To solve the problem with low complexity, this paper solve the problem by utilizing the matching theory.

We first make each source node allocate its power equally over all its occupied subcarriers. Subcarrier allocation is considered by intermediate relay. The subcarrier set and the user pair set are two disjoint sets which aim at matching with each other. The element in both sets are selfish and intelligent which aims to maximize their own interests. If subcarrier SC_k is occupied by user pair N_m, we consider the user pair N_m and the subcarrier SC_k are already paired. It is denoted as (N_m, SC_k). The conflict of interests between elements in the same set and the game between elements in different sets to maximize their own interests have a great impact on the result of the matching game. This paper use $\succ$ denote the preference relation for both subcarriers and user pairs. The preference for user pair $N_j \in N_{user}$ over the set of subcarriers is denoted as $\succ_{N_j}$. For any two subcarriers SC_k and $SC_{K'}$, $k \neq k'$, there exists two different mapping relationship ψ and ψ', satisfies $SC_k \in \psi\left(N_j\right), SC_{k'} \notin \psi\left(N_j\right), SC_{k'} \in \psi'\left(N_j\right), SC_k \notin \psi'\left(N_j\right)$. Thus, the preference for user pair over the set of subcarriers $\succ_{N_j}$ can be described as follows

$$\left(SC_k, \psi\right) \succ_{N_j} \left(SC_{k'}, \psi'\right) \Leftrightarrow R_{kj}\left(\psi\right) > R_{k'j}\left(\psi'\right), \tag{12}$$

which means that user pair N_j chooses to occupy SC_k in ψ rather than $SC_{K'}$ in ψ' because N_j can obtain higher security capacity over SC_k than over $SC_{K'}$.

Similarly, for any two subcarrier $SC_k, SC_{k'} \in K_{SC}$, $k \neq k'$, the preference for subcarriers over the subsets of users is denoted as $\succ_{SC_k}$. For two different user pair subsets U and U', $U, U' \subseteq N_{user}, U \neq U'$, there exists two different mapping relationship ψ and ψ', satisfies $U = \psi(SC_k), U' = \psi'(SC_k)$. Thus, the preference for subcarrier over the subsets of user pairs $\succ_{SC_k}$ can be described as follows

$$(U, \psi) \succ_{SC_k} (U', \psi') \Leftrightarrow R_{SC_k}(\psi) > R_{SC_k}(\psi'), \tag{13}$$

which means that subcarrier SC_k chooses to match with subset U in ψ rather than subset U' in ψ' because it can obtain higher security capacity from U'.

In the whole matching process, the user pair's preferences for subcarriers are interactional, so does the selection of subcarriers to user pairs. The algorithm procedures that update the mapping relationship between two sets depend on the structure of current matching. Every two user pairs have rights to exchange their matches in the algorithm. Therefore, this paper introduces swap matching and swap matching pairs to maximize the system security capacity.

Swap Matching. It is assume that there exists a mapping relation ψ satisfies $SC_p \in \psi(N_i), SC_q \in \psi(N_j) \&\& SC_p \notin \psi(N_j), SC_q \notin \psi(N_i)$. A swap matching is denoted as ψ_{jq}^{ip}. It is a swap operation which makes $SC_q \in \psi_{jq}^{ip}(N_i), SC_p \in \psi_{jq}^{ip}(N_j) \&\& SC_q \notin \psi_{jq}^{ip}(N_j), SC_p \notin \psi_{jq}^{ip}(N_i)$. In general, a swap matching is a operation that makes two of user pairs in the set exchange one of their occupying subcarriers and keep all other mapping relation the same.

Swap Matching Pairs. Assuming that there is a mapping relation ψ and exists a block pair (N_i, N_j) in ψ which satisfies $SC_p \in \psi(N_i)$, $SC_q \in \psi(N_j)$. If the block pair (N_i, N_j) meet the following two conditions, then (N_i, N_j) is a swap matching pair in ψ.

(i) $\forall t \in \{N_i, N_j, SC_p, SC_q\}, \left(\psi_{jq}^{ip}(t), \psi_{jq}^{ip}\right) \geq_t (\psi(t), \psi)$

(ii) $\exists t \in \{N_i, N_j, SC_p, SC_q\}, \left(\psi_{jq}^{ip}(t), \psi_{jq}^{ip}\right) \succ_t (\psi(t), \psi)$

Each user pair should find another user pair to form a swap matching pair and then swap their occupying subcarrier of the set in above inequality. For the elements in swap matching pair, they can benefit each other by swap their subcarrier without hurting the benefits of corresponding subcarriers. Then, the algorithm can obtain the optimal mapping result after multiple swap operations.

The specific details of our proposed algorithm are showed in Algorithm 1. The algorithm is divided into two parts: One is initialization and another is swap matching. First, initial mapping relation via random subcarrier allocation and each source node construct its preference matching list. Then source node keep searching its partner to form swap matching pair and change their occupying subcarrier to update matching relation ψ. The algorithm finishes until no

source node can form new swap matching pair and the optimal matching will be obtained.

Algorithm 1. Matching Subcarrier Allocation Algorithm

Input: $\mathbf{h}$, σ_n, G_k, α, N, K
Initialization
  Obtain initial mapping result based on random subcarrier allocation
    i $L(N_i), N_i \in N_{user}$
    ii $L(SC_k), SC_k \in K_{sc}$
    iii Each source node construct its preference list $P(N_i), N_i \in N_{user}$
Swap Matching
while $\exists P(N_i) \neq \emptyset, N_i \in N_{user}$ **do**
  for $i = 1 : n$ **do**
    if $P(N_i)$ is not empty **then**
      Current source node proposes itself to the most-preferred SC_k and give up SC_l
      Remove SC_k **from** $P(N_i)$
      for $j = 1 : |L(SC_k)|$ **do**
        if It's a swap matching pair **then**
          SC_k **accept the proposal**
          Update $L(N_i), N_i \in N_{user}$ **and** $L(SC_k), SC_k \in K_{sc}$
        else
          Refuse the proposal
        end if
      end for
    end if
  end for
end while
Matching Finish

3.2 Stability and Convergence

Assuming that the optimal matching mapping result ψ^* is not a stable matching. Then there exists a matching pair (N_i, SC_k), so that both N_i and SC_k can achieve higher secure transmission rates and $(N_i, SC_k) \notin \psi^*$. According to the algorithm details, N_i will propose itself to SC_k and SC_k will agree to this application, then matching switching operation will be implemented. (N_i, SC_k) is a candidate match in the iterative updating process. We assume that in the t round, SC_k discover a preferable user and delete N_i from the list, that is $\psi^t(SC_k) \succ_{SC_k} L, L \subseteq \{N_i\} \cup \psi^t(SC_k), L \subseteq \{N_i\} \cup \psi^t(SC_k), N_i \in L$. Now, a new matching relationship $\psi^t(SC_k)$ is obtained. However, $\psi^t(SC_k)$ did not survive and was replaced by the new matching relationship in the end. As for SC_k, its final matching list is $\psi(SC_k)$. Finally, we get $L \succ_{SC_k} \psi(SC_k), \psi^t(SC_k) \succ_{SC_k} L, \psi(SC_k) \succ_{SC_k} \psi^t(SC_k)$. It is contradictory to the transitive property, therefore, the hypothesis is not valid. So the matching

mapping result ψ^* is the optimal matching, the two-side matching algorithm is stable.

In each iteration process, every user node will propose itself to its favorite subcarrier. Whether the application is accepted or rejected by the subchannel, the user node will not propose itself to the same subcarrier anymore. As the iteration continues the potential choices of each user node are decreasing. For each iteration the corresponding subchannel will be removed from its preference list. The preference list of each user source node will be empty after no more than K iterations. Then the matching phase of the algorithm is over and get the optimal matching result. It proves the algorithm is convergent.

4 System Simulation

The security performance with different subcarrier allocations is shown in this section. The transmission signal is over Block Fading Channel. Users are randomly distributed in the cell. In the simulation, the peak power of each source node is 20 dBm, the path loss factor is set as 2, the cell radius is 200 m, overload coefficient in SCMA system is 2, noise variance is -174 dBm/Hz. The simulation results is obtained based on over 10000 instances of the algorithms.

We evaluate the performance of the proposed subcarrier allocation algorithm, and compare it with random subcarrier allocation and OFDMA scheme. We set the relay magnification factor as 15 dB. Figure 4 shows the relation between the total security capacity with the number of users with $d_v = 3$, and $d_f = 6$. The proposed algorithm significantly outperforms random allocation and OFDMA scheme. For optimize scheme, the total security capacity increases with the number of users, but the growth becomes slower as user number increases. That's because as the number of users increases, the candidate matching solutions go up accordingly. The proposed algorithm can converge to the optimal matching solution. Thus the security capacity continue to rise as the number of users increase. However this kind of subcarrier allocation scheme always provide services to users with better security performance. Therefore the fairness of the algorithm is poor. For OFDMA scheme, the total security capacity increases at first and then remains constant when all subcarriers are fully loaded. For random allocation scheme, its security performance is better than OFDMA scheme when the number of user is small. As the number of users increases, the total security capacity decreases even smaller than OFDMA scheme, and then remains constant when all subcarriers are fully loaded. That's because the subcarriers is not fully loaded and the interference to users is relatively small while there is few users. Compared with OFDMA users, each SCMA user can occupy more subcarriers to access to system. Therefore, the security performance of random allocation is better than OFDMA scheme when the number of users in the system is small. As the number of users becomes larger, the multiplexing users on each subcarrier increase, and then each user will suffer more severe Multi-Use interference. Since random allocation algorithm generate the result in a random way, it can't find an optimal matching solution, no security performance

gains will be obtained, even if the number of users increases. Besides the severe Multi-Use interference degrades the system security performance. Therefore, for random allocation scheme, the total security capacity decreases even smaller than OFDMA scheme as the number of users increases. If the number of system users continues to increase, all subcarriers has been fully loaded, the security performance of both schemes remain constant.

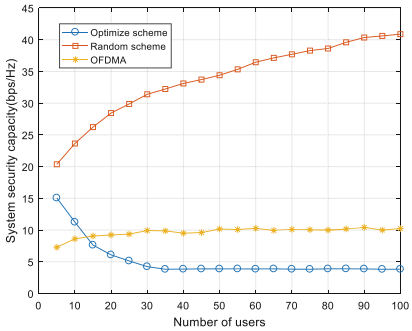

Fig. 4. Sum security capacity v.s. the number of users

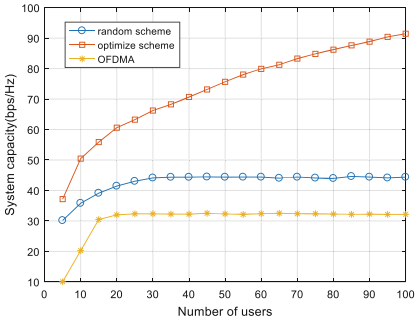

Fig. 5. Sum capacity v.s. the number of users

Figure 5 simulates the system capacity performance with three different subcarrier allocations. Simulation results indicate that the proposed subcarrier allocation scheme won't deteriorate the communication quality. It can improve both system capacity and security performance.

5 Conclusion

In this paper, we investigated the physical layer security for two-way communications with an untrusted intermediate relay in the SCMA networks. This

paper researches the subcarrier allocation problem to improve system security performance by optimizing the subcarrier assignment. The proposed subcarrier allocation algorithm can converge to an optimal matching with a low complexity and it will improve the communication quality of the system.

References

1. Nikopour, H., Baligh, H.: Sparse code multiple access. In: Proceedings of the 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), London, U.K., pp. 332–336, September 2013
2. Renfors, M., et al.: On the use of filter bank based multicarrier modulation for professional mobile radio. In: Proceedings of the 2013 IEEE 77th Vehicular Technology Conference (VTC Spring), Dresden, DE, pp. 1–5, June 2013
3. Song, G., Wang, X., Cheng, J.: Signature design of sparsely spread code division multiple access based on superposed constellation distance analysis. IEEE Access **5**, 23809–23821 (2017)
4. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
5. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
6. Csiszár, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **IT–24**, 339–348 (1978)
7. Oggier, F., Hassibi, B.: The secrecy capacity of the MIMO wiretap channel. In: Proceedings IEEE International Symposium on Information Theory (ISIT 2008), Toronto, Canada, pp. 524–528, July 2008
8. Koyluoglu, O., El-Gamal, H., Lai, L., Poor, H.V.: Interference alignment for secrecy. IEEE Trans. Inf. Theory (2008, submitted). http://arxiv.org/abs/0810.1187
9. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Secure wireless communications via cooperation. In: Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing/UIUC, Monticello, IL, pp. 1132–1138, September 2008
10. Tekin, E., Yener, A.: The general Gaussian multiple-access and twoway wiretap channels: achievable rates and cooperative jamming. IEEE Trans. Inf. Theory **54**(6), 2735–2751 (2008)
11. He, X., Yener, A.: Cooperation with an untrusted relay: a secrecy perspective. IEEE Trans. Inf. Theory **56**(8), 3807–3827 (2010)
12. Oohama, Y.: Coding for relay channels with confidential messages. In: Proceedings of the IEEE Information Theory Workshop, Cairns, Australia, pp. 87–89, September 2001
13. Oohama, Y.: Capacity theorems for relay channels with confidential messages. In: Proceedings of the IEEE International Symposium on Information Theory, Nice, France, pp. 926–930, June 2007
14. Huang, J., Mukherjee, A., Swindlehurst, A.L.: Secure communication via an untrusted non-regenerative relay in fading channels. IEEE Trans. Signal Process. **61**(10), 2536–2550 (2013)
15. He, X., Yener, A.: Two-hop secure communication using an untrusted relay. EURASIP J. Wirel. Commun. Netw. **2009**(1), 305146 (2009)
16. Di, B., Song, L., Li, Y.: Radio resource allocation for uplink sparse code multiple access (SCMA) networks using matching game. In: 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, pp. 1–6 (2016)