

Research Article

Secure Collision-Free Frequency Hopping for OFDMA-Based Wireless Networks

Leonard Lightfoot, Lei Zhang, Jian Ren, and Tongtong Li

Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI 48824, USA

Correspondence should be addressed to Tongtong Li, tongli@egr.msu.edu

Received 16 February 2009; Accepted 2 July 2009

Recommended by K. Subbalakshmi

This paper considers highly efficient antijamming system design using secure dynamic spectrum access control. First, we propose a collision-free frequency hopping (CFFH) system based on the OFDMA framework and an innovative secure subcarrier assignment scheme. The CFFH system is designed to ensure that each user hops to a new set of subcarriers in a pseudorandom manner at the beginning of each hopping period, and different users always transmit on nonoverlapping sets of subcarriers. The CFFH scheme can effectively mitigate the jamming interference, including both random jamming and follower jamming. Moreover, it has the same high spectral efficiency as that of the OFDM system and can relax the complex frequency synchronization problem suffered by conventional FH. Second, we enhance the antijamming property of CFFH by incorporating the space-time coding (STC) scheme. The enhanced system is referred to as STC-CFFH. Our analysis indicates that the combination of space-time coding and CFFH is particularly powerful in eliminating channel interference and hostile jamming interference, especially random jamming. Simulation examples are provided to illustrate the performance of the proposed schemes. The proposed scheme provides a promising solution for secure and efficient spectrum sharing among different users and services in cognitive networks.

Copyright © 2009 Leonard Lightfoot et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Mainly due to the lack of a protective physical boundary, wireless communication is facing much more serious security challenges than its wirelined counterpart. In addition to the time and frequency dispersions caused by multipath propagation and Doppler shift, wireless signals are subjected to hostile jamming/interference and interception.

Existing antijamming and anti-interception systems, including both code-division multiple access (CDMA) systems and frequency hopping (FH) systems, rely heavily on rich time-frequency diversity over large, spread spectrum. Mainly limited by multiuser interference (caused by multipath propagation and asynchronization in CDMA systems and by collision effects in FH systems), the spectral efficiency of existing jamming resistant systems is very low due to inefficient use of the large bandwidth. While these systems work reasonably well for voice centric communications which only require relatively narrow bandwidth, their low spectral efficiency can no longer provide sufficient capacity for today's high-speed multimedia wireless services. This

turns out to be the most significant obstacle in developing antijamming features for high-speed wireless communication systems, for which spectrum is one of the most precious resources. On the other hand, along with the development of wireless communications, especially cognitive radios, hostile jamming and interception are no longer limited to military applications. Therefore, a major challenge in today's wireless communications is how to design wireless systems which are highly efficient but at the same time have excellent jamming resistance properties?

In this paper, as an effort to address this problem, we propose to integrate the *frequency hopping* technique into highly efficient communication systems through a network-centric perspective. Our approach is motivated by the following observations.

(i) Orthogonal frequency division multiple access (OFDMA) is an efficient multiple user scheme that divides the entire channel into mutually orthogonal parallel subchannels. The OFDM technique transforms a frequency-selective fading channel into parallel flat fading channels. As a result, OFDM can effectively eliminate the intersymbol

interference (ISI) caused by the multipath environment and can achieve high spectral efficiency. For this reason, OFDMA has emerged as one of the prime multiple access schemes for broadband wireless networks [1, 2]. However, OFDMA does not possess any inherent security features and is fragile to hostile jamming.

(ii) FH is originally designed for jamming resistant communications. In traditional FH systems, the transmitter hops in a pseudorandom manner among available frequencies according to a prespecified algorithm; the receiver then operates in a strict synchronization with the transmitter and remains tuned to the same center frequency. Two major limitations with the conventional FH scheme are the following. (i) *Strong requirement on frequency acquisition*. In existing FH systems, exact frequency synchronization has to be kept between the transmitter and the receiver. The strict requirement on synchronization directly influences the complexity, design, and performance of the system [3], and turns out to be a significant challenge in fast hopping system design. (ii) *Low spectral efficiency over large bandwidth*. Typically, FH systems require large bandwidth, which is proportional to the hopping rate and the number of all the available channels. In conventional frequency hopping multiple access (FHMA), each user hops independently based on its own pseudorandom number (PN) sequence; a collision occurs whenever there are two users over the same frequency band. Mainly limited by the collision effect, the spectral efficiency of conventional FH systems is very low.

(iii) In literature, considerable efforts have been devoted to increasing the spectral efficiency of FH systems by applying high-dimensional modulation schemes [4–10]. More recently, a combination of the FH technique and the OFDMA system, called FH-OFDMA, has been proposed [11, 12]. However, as the system is based on the conventional FH techniques, the spectral efficiency is seriously limited by the collision effect. Along with the ever increasing demand on inherently secure high datarate wireless communications, new techniques that are more efficient and reliable have to be developed.

In this paper, we consider highly efficient antijamming system design using secure dynamic spectrum access control. First, we propose a collision-free frequency hopping (CFFH) system based on the OFDMA framework and an innovative secure subcarrier assignment scheme. The secure subcarrier assignment is achieved through an advanced encryption standard (AES) [13] based secure permutation algorithm, which is designed to ensure that (i) each user hops to a new set of subcarriers in a pseudorandom manner at the beginning of each hopping period; (ii) different users always transmit on nonoverlapping sets of subcarriers; (iii) malicious users cannot determine the hopping pattern of the authorized users and hence cannot launch follower jamming attacks. (Follower jamming is the worst jamming scenario, in which the attacker is aware of the carrier frequency or the frequency hopping pattern of an authorized user and can destroy the user's communication by launching jamming interference over the same frequency bands.) In other words, the proposed CFFH scheme can effectively mitigate jamming interference, including both random jamming and follower

jamming. Moreover, using the fast Fourier transform (FFT) based OFDMA framework, CFFH has the same high spectral efficiency as that of OFDM and at the same time can relax the complex frequency synchronization problem suffered by conventional FH systems.

We further enhance the antijamming property of CFFH by incorporating the space-time coding (STC) scheme. Space-time block coding, which was first proposed by Alamouti [14] and refined by Tarokh et al. [15, 16], is a technique that exploits antenna array spatial diversity to provide gains against fading environments. When incorporated with OFDM, the space-time diversity in space-time coding is then converted to space-frequency diversity. The combination of space-time coding and CFFH is found to be particularly powerful in eliminating channel interference and hostile jamming interference, especially random jamming. In this paper, we analyze the performance of the proposed STC-CFFH system through the following aspects: (i) comparing the spectral efficiency of the proposed scheme with that of the conventional FH-OFDMA system and (ii) investigating the performance of the STC-CFFH system under Rayleigh fading with hostile jamming. Our analysis indicates that the proposed system is both highly efficient and very robust under jamming environments.

Due to its high spectral efficiency, OFDMA has turned out to be a prime multiple access scheme for dynamic spectrum access network enabled by cognitive radios and/or software defined radios. By allowing the users to hop over multiple OFDM bands, the OFDMA-based dynamic spectrum access control scheme proposed in this paper can be applied directly to broadband wireless systems that consists of a large number of OFDM bands and hence provides a promising and flexible solution for secure and efficient spectrum sharing among different users and services in cognitive networks.

This paper is organized as follows. In Section 2, the innovative secure subcarrier assignment algorithm is introduced. In Section 3, the proposed collision-free frequency hopping scheme is presented. The antijamming features of the proposed CFFH scheme are enhanced with space-time coding in Section 4. The spectral efficiency and jamming resistant properties of the proposed systems are analyzed in Section 5. Simulation examples are provided in Section 6. Finally, conclusions are drawn in Section 7.

2. Secure Subcarrier Assignment

In this section, we present the proposed secure subcarrier assignment scheme, for which the major component is an AES-based secure permutation algorithm. AES is chosen because of its simplicity of design, variable block and key sizes, feasibility in both hardware and software, and resistance against all known attacks [17]. Note that the secure subcarrier assignment is not limited to any particular cryptographic algorithm, but it is highly recommended that only thoroughly analyzed cryptographic algorithms are applied.

The AES-based permutation algorithm is used to securely select the frequency hopping pattern for each user so that: (i) different users always transmit on nonoverlapping sets

of subcarriers; (ii) malicious users cannot determine the frequency hopping pattern and therefore cannot launch follower jamming attacks.

We assume that there is a total of N_c available subcarriers, and there are M users in the system. For $i = 0, 1, \dots, M - 1$, the number of subcarriers assigned to user i is denoted as N_u^i . We assume that different users transmit over nonoverlapping set of subcarriers, and we have $\sum_{i=0}^{M-1} N_u^i = N_c$. The secure subcarrier assignment algorithm is described in the following subsections.

2.1. Secure Permutation Index Generation. A pseudorandom binary sequence is generated using a 32-bit linear feedback shift register (LFSR), which is initialized by a secret sequence chosen by the base station. The LFSR has the following characteristic polynomial:

$$\begin{aligned} x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11}, \\ + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1. \end{aligned} \quad (1)$$

Use the pseudorandom binary sequence generated by the LFSR as the plaintext. Encrypt the plaintext using the AES algorithm and a secure key. The key size can be 128, 192, or 256. The encrypted plaintext is known as the ciphertext. Assume N_c is a power of 2; pick an integer $L \in [N_c/2, N_c]$. Note that a total of $N_b = \log_2 N_c$ bits are required to represent each subcarrier, and let $q = L \log_2 N_c$. Take q bits from the ciphertext and put them as a q -bit vector $\mathbf{e} = [e_1, e_2, \dots, e_q]$.

Partition the ciphertext sequence \mathbf{e} into L groups, such that each group contains N_b bits. For $k = 1, 2, \dots, L$, the partition of the ciphertext is as follows:

$$\mathbf{p}_k = [e_{(k-1)*N_b+1}, e_{(k-1)*N_b+2}, \dots, e_{(k-1)*N_b+N_b}], \quad (2)$$

where \mathbf{p}_k corresponds to the k th N_b -bit vector.

For $k = 1, 2, \dots, L$, denote P_k as the decimal number corresponding to \mathbf{p}_k , that is,

$$\begin{aligned} P_k = e_{(k-1)*N_b+1} \cdot 2^{N_b-1} + e_{(k-1)*N_b+2} \cdot 2^{N_b-2} \\ + \dots + e_{(k-1)*N_b+N_b-1} \cdot 2^1 \\ + e_{(k-1)*N_b+N_b} \cdot 2^0. \end{aligned} \quad (3)$$

Finally, we denote $P = [P_1, P_2, \dots, P_L]$ as the permutation index vector. Here the largest number in P is $N_c - 1$. In the following subsection, we will discuss the secure permutation algorithm.

2.2. Secure Permutation Algorithm and Subcarrier Assignment. For $k = 0, 1, 2, \dots, L$, denote $I_k = [I_k(0), I_k(1), \dots, I_k(N_c - 1)]$ as the index vector at the k th step. The secure permutation scheme of the index vector is achieved through the following steps.

Step 0. Initially, the index vector is $I_0 = [I_0(0), I_0(1), \dots, I_0(N_c - 1)]$, and the permutation index is $P = [P_1, P_2, \dots, P_L]$. We start with $I_0 = [0, 1, \dots, N_c - 1]$.

Step 1. For $k = 1$, switch $I_0(0)$ and $I_0(P_1)$ in index vector I_0 to obtain I_1 . In other words, $I_1 = [I_1(0), I_1(1), \dots, I_1(N_c - 1)]$, where $I_1(0) = I_0(P_1)$, $I_1(P_1) = I_0(0)$, and $I_1(m) = I_0(m)$ for $m \neq 0, P_1$.

Step 2. Repeat the previous step for $k = 2, 3, \dots, L$. In general, if we already have $I_{k-1} = [I_{k-1}(0), I_{k-1}(1), \dots, I_{k-1}(N_c - 1)]$, then we can obtain $I_k = [I_k(0), I_k(1), \dots, I_k(N_c - 1)]$ through the permutation defined as $I_k(k - 1) = I_{k-1}(P_k)$, $I_k(P_k) = I_{k-1}(k - 1)$, and $I_k(m) = I_{k-1}(m)$ for $m \neq k - 1, P_k$.

Step 3. After L steps, we obtain the subcarrier frequency vector as $F_L = [f_{L(0)}, f_{L(1)}, \dots, f_{L(N_c-1)}]$.

Step 4. The subcarrier frequency vector F_L is used to assign subcarriers to the users. Recall that, for user $i = 0, 1, \dots, M - 1$, the total number of subcarriers assigned to the i th user is N_u^i . We assign subcarriers $\{f_{L(0)}, f_{L(1)}, \dots, f_{L(N_u^i-1)}\}$ to user 0; assign $\{f_{L(N_u^0)}, f_{L(N_u^0+1)}, \dots, f_{L(N_u^0+N_u^1-1)}\}$ to user 1, and so on.

Proposition 1. *The proposed secure subcarrier assignment scheme ensures non-overlapping transmission among all the users in the system.*

Proof. In fact, after L steps, we obtain the subcarrier frequency vector as $F_L = [f_{L(0)}, f_{L(1)}, \dots, f_{L(N_c-1)}]$. We can rewrite the subcarrier frequency vector F_L as $F_L = [F_L(0), F_L(1), \dots, F_L(N_c - 1)]$ by defining $F_L(j) = f_{L(j)}$ for $j = 0, 1, \dots, N_c - 1$, where N_c is the total number of subcarriers. Assume that we have M users in the system, and for $i = 0, 1, \dots, M - 1$, the total number of subcarriers assigned to the i th user is N_u^i . The subcarrier assignment process described in Step 4 of the secure subcarrier algorithm above is equivalent to assigning subcarriers $\{F_L(0), F_L(1), \dots, F_L(N_u^0 - 1)\}$ to user 0, and subcarriers $\{F_L(N_u^0), F_L(N_u^0 + 1), \dots, F_L(N_u^0 + N_u^1 - 1)\}$ to user 1, and so on.

Because each frequency index appears in F_L once and only once, the proposed algorithm ensures that (i) all the users are transmitting on non-overlapping sets of subcarriers; (ii) no subcarrier is left idle. That is, all the subcarriers are active. \square

The secure permutation index generation is performed at the base station. The base station sends encrypted channel assignment information to each user periodically through the control channels.

The proposed scheme addresses the problem of securely allocating subcarriers in the presence of hostile jamming. This algorithm can be combined with existing resource allocation techniques. First, the number of subcarriers assigned to each user can be determined through power and bandwidth optimization; see [11, 18], for example. Then, we use the secure subcarrier assignment algorithm to select the group of subcarriers for each user at each hopping period. In the following, we illustrate the secure subcarrier assignment algorithm through a simple example.

Example 1. Assume that the total number of available subcarriers is $N_c = 8$, to be equally divided among $M = 2$

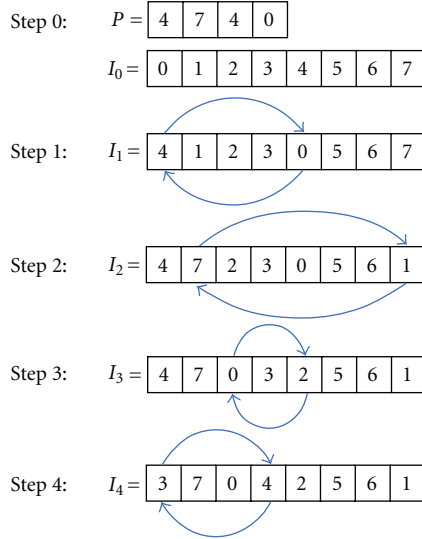


FIGURE 1: Example of the secure permutation algorithm for $N_c = 8$ subcarriers and $M = 2$ users.

users; the permutation index vector $P = [4, 7, 4, 0]$, and the initial index vector $I_0 = [0, 1, 2, 3, 4, 5, 6, 7]$, as shown in Figure 1. Note that, the initial index vector I_0 can contain any random permutation of the sequence $\{0, 1, \dots, N_c - 1\}$ and $L \in [N_c/2, N_c]$. In this example, we choose $L = N_c/2$.

At Step 1, $k = 1$, and $P_k = 4$, thus we switch $I_0(P_k)$ and $I_0(k-1)$ of the index vector I_0 . After the switching, we obtain a new index vector $I_1 = [4, 1, 2, 3, 0, 5, 6, 7]$.

At Step 2, $k = 2$, and $P_k = 7$, thus we switch $I_1(P_k)$ and $I_1(k-1)$ of the index vector I_1 . We obtain the new index vector $I_2 = [4, 7, 2, 3, 0, 5, 6, 1]$. Below are the remaining index vectors for $k = 3, 4$:

$$I_3 = [4, 7, 0, 3, 2, 5, 6, 1], \quad I_4 = [3, 7, 0, 4, 2, 5, 6, 1]. \quad (4)$$

The subcarrier frequency vector is $F_4 = [f_{I_4(0)}, f_{I_4(1)}, \dots, f_{I_4(N_c-1)}]$. Frequencies $\{f_3, f_7, f_0, f_4\}$ are assigned to user 0, and frequencies $\{f_2, f_5, f_6, f_1\}$ are assigned to user 1.

In the following section, we will introduce the proposed CFFH system.

3. The Collision-Free Frequency Hopping (CFFH) Scheme

The CFFH system is essentially an OFDMA system equipped with secure FH-based dynamic spectrum access control, where the hopping pattern is determined by the secure subcarrier assignment algorithm described in the previous section.

3.1. Signal Transmission. Consider a system with M users, utilizing an OFDM system with N_c subcarriers, $\{f_0, \dots, f_{N_c-1}\}$. At each hopping period, each user is assigned a specific subset of the total available subcarriers. One hopping period may last one or more OFDM symbol periods. Assuming that at the n th symbol, user i has been assigned a

set of subcarriers $C_{n,i} = \{f_{n,i_0}, \dots, f_{n,i_{N_u^i-1}}\}$; that is, user i will transmit and only transmit on these subcarriers. Here N_u^i is the total number of subcarrier assigned to user i . Note that for any n ,

$$C_{n,i} \cap C_{n,j} = \emptyset, \quad \text{if } i \neq j. \quad (5)$$

That is, users transmit on non-overlapping subcarriers. In other words, there is no collision between the users. Ideally, for full capacity of the OFDM system,

$$\bigcup_{i=0}^{M-1} C_{n,i} = \{f_0, \dots, f_{N_c-1}\}. \quad (6)$$

For the i th user, if $N_u^i > 1$, then the i th users information symbols are first fed into a serial-to-parallel converter. Assuming that at the n th symbol period, user i transmits the information symbols $\{u_{n,0}^{(i)}, \dots, u_{n,N_u^i-1}^{(i)}\}$ (which are generally QAM symbols) through the subcarrier set $C_{n,i} = \{f_{n,i_0}, \dots, f_{n,i_{N_u^i-1}}\}$. User i 's transmitted signal at the n th OFDM symbol can then be written as

$$s_n^{(i)}(t) = \sum_{l=0}^{N_u^i-1} u_{n,l}^{(i)} e^{j2\pi f_{n,l} t}. \quad (7)$$

Note that each user does not transmit on subcarriers which are not assigned to him/her, by setting the symbols to zeros over these subcarriers. This process ensures collision-free transmission among the users.

3.2. Signal Detection. At the receiver, the received signal is a superposition of the signals transmitted from all users:

$$r(t) = \sum_{i=0}^{M-1} r_n^{(i)}(t) + n(t), \quad (8)$$

where

$$r_n^{(i)}(t) = s_n^{(i)}(t) * h_i(t), \quad (9)$$

and $n(t)$ is the additive noise. In (9), $h_i(t)$ is the channel impulse response corresponding to user i . Note that in OFDM systems, guard intervals are inserted between symbols to eliminate intersymbol interference (ISI); so it is reasonable to study the signals in a symbol-by-symbol manner. Equations (7)–(9) represent an uplink system. The downlink system can be formulated in a similar manner.

As is well known, the OFDM transmitter and receiver are implemented through IFFT and FFT, respectively. Denoting the $N_c \times 1$ symbol vector corresponding to user i 's n th OFDM symbol as $\mathbf{u}_n^{(i)}$, we have

$$\mathbf{u}_n^{(i)}(l) = \begin{cases} 0, & l \notin \{i_0, \dots, i_{N_u^i-1}\}, \\ u_{n,l}^{(i)}, & l \in \{i_0, \dots, i_{N_u^i-1}\}. \end{cases} \quad (10)$$

Let T_s denote the OFDM symbol period. The discrete form of the transmitted signal $s_n^{(i)}(t)$ (sampled at lT_s/N_c) is

$$\mathbf{s}_n^{(i)} = \mathbf{F} \mathbf{u}_n^{(i)}, \quad (11)$$

where \mathbf{F} is the IFFT matrix defined as

$$\mathbf{F} = \frac{1}{\sqrt{N_c}} \begin{pmatrix} W_{N_c}^{00} & \cdots & W_{N_c}^{0(N_c-1)} \\ \vdots & \ddots & \vdots \\ W_{N_c}^{(N_c-1)0} & \cdots & W_{N_c}^{(N_c-1)(N_c-1)} \end{pmatrix}, \quad (12)$$

with $W_{N_c}^{nk} = e^{j2\pi nk/N_c}$. As we only consider one OFDM symbol at a time, for notation simplification, here we omit the insertion of the guard interval (i.e., the cyclic prefix which is used to ensure that there is no ISI between two successive OFDM symbols).

Let $\mathbf{h}_i = [h_i(0), \dots, h_i(N_c - 1)]$ be the discrete channel impulse response vector, and let

$$\mathbf{H}_i = \mathbf{F}\mathbf{h}_i \quad (13)$$

be the Fourier transform of \mathbf{h}_i . Then the received signal corresponding to user i is

$$\mathbf{r}_n^{(i)}(l) = \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l). \quad (14)$$

The overall received signal is then given by

$$\begin{aligned} \mathbf{r}_n(l) &= \sum_{i=0}^{M-1} \mathbf{r}_n^{(i)}(l) + \mathbf{N}_n(l) \\ &= \sum_{i=0}^{M-1} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l) + \mathbf{N}_n(l), \end{aligned} \quad (15)$$

where $\mathbf{N}_n(l)$ is the Fourier transform of the noise corresponding to the n th OFDM symbol.

Note that due to the collision-free subcarrier assignment, for each l , there is at most one nonzero item in the sum $\sum_{i=0}^{M-1} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l)$. As a result, standard channel estimation algorithms and signal detection algorithms for OFDM systems can be implemented. In fact, each user can send pilot symbols on its subcarrier set to perform channel estimation. It should be pointed out that instead of estimating the whole frequency domain channel vector \mathbf{H}_i , for signal recovery, user i only needs to estimate the entries corresponding to its subcarrier set, that is, the values of $\mathbf{H}_i(l)$ for $l \in \{i_0, \dots, i_{N_u^i-1}\}$. After channel estimation, user i 's information symbols can be estimated from

$$\mathbf{u}_n^{(i)}(l) = \frac{\mathbf{r}_n^{(i)}(l)}{\mathbf{H}_i(l)}, \quad l \in \{i_0, \dots, i_{N_u^i-1}\}. \quad (16)$$

It is also interesting to note that we can obtain adequate channel information from all the users simultaneously, which can be exploited for dynamic resource reallocation to achieve better BER performance and real-time jamming prevention.

4. Space-Time-Coded Collision-Free Frequency Hopping

In this section, we consider to enhance the antijamming features of the CFFH scheme using space-time coding. Here we present the transmitter and receiver design of the proposed STC-CFFH system from the downlink perspective. The uplink can be designed in a similar manner.

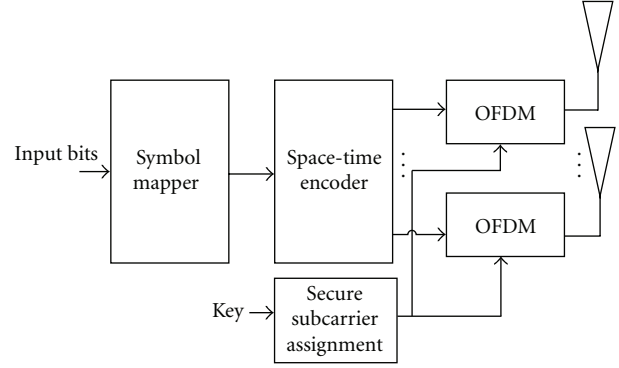


FIGURE 2: Block diagram of the STC-CFFH transmitter.

4.1. Transmitter Design. We assume that, during each hopping period, the number of subcarriers assigned to each user in the CFFH system is fixed. Recall that one hopping period may contain one or more OFDM symbol periods. In the following we illustrate the transmitter design over one OFDM symbol.

Assume that the transmitter at the base station has n_T antennas, and there are M users in the system. Over each OFDM symbol period, the i th user is assigned N_u^i subcarriers, which do not need to be contiguous. The transmitter structure at the base station is illustrated in Figure 2.

Initially, the input bit stream corresponding to each user is mapped to symbols based on a selected constellation. The constellation could be different for different users based on the channel condition and user data rate [19, 20]. Assume the base station uses an $n_T \times n_T$ space-time block code (STBC). Note that nonsquare STBC codes [15, 16] exist, but for notation simplicity, here we adopt the $n_T \times n_T$ square code. For each user, divide the N_u^i subcarriers into $G_i = N_u^i/n_T$ groups, where each group contains n_T subcarriers, which is of the same length as that of the STBC. For simplicity, we assume that G_i is an integer; that is, each user transmits G_i space-time blocks in one OFDM symbol period. (Otherwise, if G_i is not an integer, the symbols can be broken down and transmitted over two successive OFDM symbol periods.)

For each $n \in \{1, 2, \dots, G_i\}$, the base station takes a block of n_T complex symbols and maps them to a $n_T \times n_T$ STBC code matrix $X_i(n)$. In other words, for $n = 1, 2, \dots, G_i$, $m = 1, 2, \dots, n_T$, the m th row of the code matrix $X_i(n)$ is merged with the corresponding symbols from other users and transmitted through the m th transmit antenna, and all symbols within each column ($m = 1, 2, \dots, n_T$) of the code matrix $X_i(n)$ are transmitted over the same subcarrier. The code matrix $X_i(n)$ is given by

$$X_i(n) = \begin{matrix} \text{Subcarrier} \longrightarrow \\ \begin{bmatrix} x_{i,1}^1(n) & \cdots & x_{i,n_T}^1(n) \\ \vdots & \ddots & \vdots \\ x_{i,1}^{n_T}(n) & \cdots & x_{i,n_T}^{n_T}(n) \end{bmatrix} \\ \downarrow \text{Antenna,} \end{matrix} \quad (17)$$

TABLE 1: STC-CFFH transmitter example.

Tx	freq.							
	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
1	$x_{0,1}(1)$	$x_{1,1}(1)$	$-x_{1,2}^*(1)$	$-x_{0,2}^*(1)$	$x_{0,1}(2)$	$x_{1,1}(2)$	$-x_{1,2}^*(2)$	$-x_{0,2}^*(2)$
2	$x_{0,2}(1)$	$x_{1,2}(1)$	$x_{1,1}^*(1)$	$x_{0,1}^*(1)$	$x_{0,2}(2)$	$x_{1,2}(2)$	$x_{1,1}^*(2)$	$x_{0,1}^*(2)$

where $x_{i,t}^m(n)$ is the t th symbol of the n th block for user i in transmit antenna m .

Note that since each user is assigned multiple frequency bands, we are transmitting symbols over multiple subcarriers instead of multiple time slots. Thus the time diversity of the space-time coder is converted to frequency diversity, and this structure is referred to as space-frequency coding [21].

STC-CFFH Transmitter Design Example. We provide an example to illustrate the transmitter structure of STC-CFFH, in which the subcarrier assignment is based on the example in Section 2. Assume an Alamouti space-time coded system with $n_T = 2$ and we have $M = 2$ users. A total of $N_c = 8$ subcarriers are available, and each user is assigned $N_u^0 = N_u^1 = 4$ subcarriers. For this example, each user transmits $G_i = N_u^i/n_T = 2$ code matrices in one OFDM symbol period. Consider the n th block for the i th user, where $n = 1, 2$ in this case. The space-time encoder takes $n_T = 2$ complex symbols $x_{i,1}(n), x_{i,2}(n)$ in each encoding operation and maps them to the code matrix $X_i(n)$. In this example, the first and second rows of $X_i(n)$ will be sent from the first and second transmit antennas, respectively.

In this example, we can drop the superscript m in $x_{i,t}^m(n)$ by representing $X_i(n)$ with the Alamouti space-time code block structure [14]. Then the code matrices $X_i(n)$ are given by

$$\begin{array}{c} \text{Subcarrier} \longrightarrow \\ X_i(n) = \begin{bmatrix} x_{i,1}(n) & -x_{i,2}^*(n) \\ x_{i,2}(n) & x_{i,1}^*(n) \end{bmatrix} \quad \downarrow \text{Antenna,} \end{array} \quad (18)$$

where $*$ is the complex conjugate operator. Specifically, User 0's two code matrices are represented as

$$\begin{aligned} X_0(1) &= \begin{bmatrix} x_{0,1}(1) & -x_{0,2}^*(1) \\ x_{0,2}(1) & x_{0,1}^*(1) \end{bmatrix}, \\ X_0(2) &= \begin{bmatrix} x_{0,1}(2) & -x_{0,2}^*(2) \\ x_{0,2}(2) & x_{0,1}^*(2) \end{bmatrix}, \end{aligned} \quad (19)$$

and User 1's two code matrices are represented as

$$\begin{aligned} X_1(1) &= \begin{bmatrix} x_{1,1}(1) & -x_{1,2}^*(1) \\ x_{1,2}(1) & x_{1,1}^*(1) \end{bmatrix}, \\ X_1(2) &= \begin{bmatrix} x_{1,1}(2) & -x_{1,2}^*(2) \\ x_{1,2}(2) & x_{1,1}^*(2) \end{bmatrix}. \end{aligned} \quad (20)$$

Recall the secure subcarrier assignment from the example in Section 2. User 0 is assigned to subcarriers $\{f_0, f_3, f_4, f_7\}$.

User 1 is assigned to subcarriers $\{f_1, f_2, f_5, f_6\}$. A depiction of the subcarrier allocation for this example is provided in Table 1.

For user 0, $[x_{0,1}(1), -x_{0,2}^*(1), x_{0,1}(2), -x_{0,2}^*(2)]$ is transmitted through antenna 1 over subcarriers $\{f_0, f_3, f_4, f_7\}$, respectively; $[x_{0,2}(1), x_{0,1}^*(1), x_{0,2}(2), x_{0,1}^*(2)]$ is transmitted through antenna 2 over the same group of subcarriers. User 1's subcarrier allocation can be achieved in the same manner as User 0.

4.2. Receiver Design. Assume that user i has n_R antennas. Recall that the secure permutation index generation is performed at the base station, and the base station sends encrypted channel assignment information to each user periodically through the control channels. After cyclic prefix removal and FFT, the receiver will only extract the symbols on the subcarriers assigned to itself and discard the symbols on the rest of subcarriers. The extracted symbols are reorganized into a $n_R \times n_T$ matrix $R_i(n)$, which corresponds to the transmitted code matrix $X_i(n)$. Thus the space-time decoding can be performed for each symbol matrix $R_i(n)$ individually, and the estimated symbols are mapped back into bits by the symbol demapper.

Here we consider the space-time decoding algorithm for a single symbol matrix $R_i(n)$ given as

$$\begin{array}{c} \text{Subcarrier} \longrightarrow \\ R_i(n) = \begin{bmatrix} r_{i,1}^1(n) & \cdots & r_{i,n_T}^1(n) \\ \vdots & \ddots & \vdots \\ r_{i,1}^{n_R}(n) & \cdots & r_{i,n_T}^{n_R}(n) \end{bmatrix} \quad \downarrow \text{Antenna,} \end{array} \quad (21)$$

where $r_{i,t}^j(n)$ is the t th symbol of group n for user i from j th receive antenna. Each symbol in the matrix $R_i(n)$ can be obtained as

$$r_{i,t}^j(n) = \sum_{m=1}^{n_T} H_{i,t}^{j,m}(n) x_{i,t}^m(n) + n_{i,t}^j(n), \quad (22)$$

where $H_{i,t}^{j,m}(n)$ is the channel frequency response for the path from the m th transmit antenna to the j th receive antenna corresponding to t th symbol of group n for user i . It is assumed that the channels between the different antennas are uncorrelated. Here, $n_{i,t}^j(n)$ is the OFDM-demodulated version of the additive white Gaussian noise (AWGN) at the j th receive antenna for t th symbol of the n th group for i th user. The noise is assumed to be zero-mean with variance σ_N^2 .

TABLE 2: STC-CFFH receiver example.

Rx	freq.							
	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
1	$r_{0,1}^1(1)$	$r_{1,1}^1(1)$	$r_{1,2}^1(1)$	$r_{0,2}^1(1)$	$r_{0,1}^1(2)$	$r_{1,1}^1(2)$	$r_{1,2}^1(2)$	$r_{0,2}^1(2)$
2	$r_{0,1}^2(1)$	$r_{1,1}^2(1)$	$r_{1,2}^2(1)$	$r_{0,2}^2(1)$	$r_{0,1}^2(2)$	$r_{1,1}^2(2)$	$r_{1,2}^2(2)$	$r_{0,2}^2(2)$

The space-time maximum likelihood (ML) decoder is obtained as

$$\hat{X}_i(n) = \arg \min_{X_i(n)} \sum_{j=1}^{n_R} \sum_{t=1}^{n_T} \left| r_{i,t}^j(n) - \sum_{m=1}^{n_T} H_{i,t}^{j,m}(n) x_{i,t}^m(n) \right|^2, \quad (23)$$

where $\hat{X}_i(n)$ denotes the recovered symbols of group n for user i . Note that the minimization is performed over all possible space-time codewords.

STC-CFFH Receiver Design Example. We continue with the transmitter example in the previous subsection. Assuming that each user is equipped with $n_R = 2$ receive antennas, the received symbols are illustrated in Table 2. Arranging the extracted symbols according to the users and the groups, the extracted symbol matrix $R_i(n)$ is given as

$$\begin{array}{c} \text{Subcarrier} \longrightarrow \\ R_i(n) = \begin{bmatrix} r_{i,1}^1(n) & r_{i,2}^1(n) \\ r_{i,1}^2(n) & r_{i,2}^2(n) \end{bmatrix} \quad \downarrow \text{Antenna.} \end{array} \quad (24)$$

Specifically, User 0's two extracted symbol matrices can be represented as

$$\begin{aligned} R_0(1) &= \begin{bmatrix} r_{0,1}^1(1) & r_{0,2}^1(1) \\ r_{0,1}^2(1) & r_{0,2}^2(1) \end{bmatrix}, \\ R_0(2) &= \begin{bmatrix} r_{0,1}^1(2) & r_{0,2}^1(2) \\ r_{0,1}^2(2) & r_{0,2}^2(2) \end{bmatrix}, \end{aligned} \quad (25)$$

and User 1's two extracted symbol matrices can be represented as

$$\begin{aligned} R_1(1) &= \begin{bmatrix} r_{1,1}^1(1) & r_{1,2}^1(1) \\ r_{1,1}^2(1) & r_{1,2}^2(1) \end{bmatrix}, \\ R_1(2) &= \begin{bmatrix} r_{1,1}^1(2) & r_{1,2}^1(2) \\ r_{1,1}^2(2) & r_{1,2}^2(2) \end{bmatrix}. \end{aligned} \quad (26)$$

Then, the ML space-time decoding is performed for each $R_i(n)$.

Remark 1. In the discussion above, we focused on STC-CFFH system for the downlink case, where the information is transmitted from base station to the multiple users. In the uplink case, the secure permutation index is encrypted and transmitted from base station to each user, prior to the user transmission. Then during the transmission, each user

only transmits on the subcarriers assigned to him/her. The receiver at the base station separates each user's transmitted data. In order for the user to use space-time coding, each user needs to have at least two antennas.

5. Performance Analysis of STC-CFFH

In this section, we investigate the spectral efficiency and the performance of the proposed schemes under jamming interference over frequency selective fading environments. First, the system performance in jamming-free case is analyzed. Second, the system performance under hostile jamming is investigated. Finally, the spectral efficiency comparison of the proposed schemes and the conventional FH-OFDMA system is performed.

5.1. System Performance in Jamming-Free Case. First, we analyze the pairwise error probability of the STC-CFFH system under Rayleigh fading. Assume ideal channel state information (CSI) and perfect synchronization between transmitter and receiver. Recall that the ML space-time decoding rule for the extracted symbol matrix $R_i(n)$ is given by (23).

Denote the pairwise error probability of transmitting $X_i(n)$ and deciding in favor of another codeword $\hat{X}_i(n)$, given the realizations of the fading channel $H_{i,t}^{j,m}(n)$, as $P(X_i(n), \hat{X}_i(n) | H_{i,t}^{j,m}(n))$. This pairwise error probability is bounded by [22, see page 255]

$$P(X_i(n), \hat{X}_i(n) | H_{i,t}^{j,m}(n)) \leq \exp\left(-d^2(X_i(n), \hat{X}_i(n)) \frac{E_s}{4N_0}\right), \quad (27)$$

where E_s is the average symbol energy, N_0 is the noise power spectral density, and $d^2(X_i(n), \hat{X}_i(n))$ is a modified Euclidean distance between the two space-time codewords $X_i(n)$ and $\hat{X}_i(n)$ and is given by

$$d^2(X_i(n), \hat{X}_i(n)) = \sum_{t=1}^{n_T} \sum_{j=1}^{n_R} \left| \sum_{m=1}^{n_T} H_{i,t}^{j,m}(n) (\hat{x}_{i,t}^m(n) - x_{i,t}^m(n)) \right|^2, \quad (28)$$

where $\hat{x}_{i,t}^m(n)$ is the estimated version of $x_{i,t}^m(n)$.

Let us define a codeword difference matrix $C(X_i(n), \hat{X}_i(n)) = X_i(n) - \hat{X}_i(n)$ and define a codeword distance matrix $B(X_i(n), \hat{X}_i(n))$ with rank r_B as

$$B(X_i(n), \hat{X}_i(n)) = C(X_i(n), \hat{X}_i(n)) \cdot C(X_i(n), \hat{X}_i(n))^H, \quad (29)$$

where H denotes the Hermitian operator. Since the matrix $B(X_i(n), \hat{X}_i(n))$ is a nonnegative definite Hermitian matrix, the eigenvalues of $B(X_i(n), \hat{X}_i(n))$ are nonnegative real numbers, denoted as $\lambda_1, \lambda_2, \dots, \lambda_{r_B}$.

After averaging with respect to the Rayleigh fading coefficients, the upper bound of pairwise error probability can be obtained as [23]

$$P(X_i(n), \hat{X}_i(n) | H_{i,t}^{j,m}(n)) \leq \left(\prod_{j=1}^{r_B} \lambda_j \right)^{-n_R} \left(\frac{E_s}{4N_0} \right)^{-r_B n_R}. \quad (30)$$

In the case of low signal-to-noise ratio (SNR), the upper bound in (30) can be expressed as [22],

$$P(X_i(n), \hat{X}_i(n) | H_{i,t}^{j,m}(n)) \leq \left(1 + \frac{E_s}{4N_0} \sum_{j=1}^{r_B} \lambda_j \right)^{-n_R}. \quad (31)$$

5.2. System Performance under Hostile Jamming. In this subsection, we will first introduce the jamming models, and then analyze the system performance under both full-band jamming and partial-band jamming.

5.2.1. Jamming Models. Jamming interference in the OFDM framework can severely degrade the system performance [24]. Each extracted symbol in the matrix $R_i(n)$ that experiences jamming interference is given as

$$r_{i,t}^j(n) = \sum_{m=1}^{n_T} H_{i,t}^{j,m}(n) x_{i,t}^m(n) + n_{i,t}^j(n) + J_{i,t}^j(n), \quad (32)$$

where $J_{i,t}^j(n)$ is the jamming interference at the j th receive antenna for t th symbol of the n th group for i th user. Assume that all jamming interference $J_{i,t}^j(n)$ has the same power spectral density N_J , then the signal-to-jamming plus noise ratio (SJNR) at the receiver is represented by $\text{SJNR} = E_s / (N_0 + N_J)$. When the noise is dominated by jamming, the SJNR can be represented as the signal-to-jamming ratio (SJR) where $\text{SJR} = E_s / N_J$.

Partial-band jamming [25–27] is generally characterized by the additive Gaussian noise interference with flat power spectral density N_J/ρ over a fraction ρ of the total bandwidth and negligible interference over the remaining fraction $(1-\rho)$ of the band. ρ is also referred to as the jammer occupancy and is given as

$$\rho = \frac{W_J}{W_S} \leq 1, \quad (33)$$

where W_J is the jamming bandwidth, and W_S is the total signal bandwidth. For CFFH, partial-band jamming means that the jamming power is concentrated on a certain group of subcarriers. Let n_j denote the number of jammed subcarriers, then the jamming ratio ρ is given by $\rho = n_j/n_T$. For a particular code matrix $X_i(n)$, this means that on average, ρn_T subcarriers are jammed out of n_T subcarriers used by $X_i(n)$.

When $\rho = 1$, the jamming power is uniformly distributed over the entire bandwidth. In this case, the partial-band

jamming becomes *full-band jamming* [28, 29]. For a CFFH system, full-band jamming means that the jamming power is uniformly distributed over all N_c .

5.2.2. System Performance under Rayleigh Fading and Full-Band Jamming. In the presence of Rayleigh fading and full-band jamming, the pairwise error probability can be expressed in terms of the jamming power spectral density N_J and average signal power E_s . In the case of high SNR, the upper bound in (30) can be expressed as

$$P(X_i(n), \hat{X}_i(n) | H_{i,t}^{j,m}(n)) \leq \left(\prod_{j=1}^{r_B} \lambda_j \right)^{-n_R} \left(\frac{E_s}{4N_J} \right)^{-r_B n_R}. \quad (34)$$

From (31), the upper bound in the presence of Rayleigh fading and full-band jamming can be expressed as

$$P(X_i(n), \hat{X}_i(n) | H_{i,t}^{j,m}(n)) \leq \left(1 + \frac{E_s}{4(N_0 + N_J)} \sum_{j=1}^{r_B} \lambda_j \right)^{-n_R}. \quad (35)$$

As will be confirmed in Section 6: for the STC-CFFH system, the space-frequency diversity gain is insignificant at low SJNR; however, the diversity gain becomes noticeable at high SJNR.

5.2.3. System Performance under Rayleigh Fading and Partial-Band Jamming. Recall that each column of the received symbol matrix $R_i(n)$ is obtained from the same subcarrier in all received antennas. When we have partial-band jamming, most likely not all columns of $R_i(n)$ are jammed, since each column is transmitted through different subcarriers. Thus the receiver may be able to recover the transmitted signal relying on the jamming-free columns.

Orthogonal space-time codes (OSTCs) are capable of perfectly decoding the transmitted symbols under partial-band jamming and noise-free environments when at least one frequency band is not jammed. We consider a $n_T = 4$ space-time orthogonal block code design as an example. Following the same notation convention in the STC-CFFH transmitter example in Section 4, the code matrix with transmit symbols $x_{i,t}(n)$ for $t = 1, 2, 3, 4$, is represented as

$$X_i(n) = \begin{bmatrix} x_{i,1}(n) & x_{i,2}(n) & x_{i,3}(n) & x_{i,4}(n) \\ -x_{i,2}(n) & x_{i,1}(n) & -x_{i,4}(n) & x_{i,3}(n) \\ -x_{i,3}(n) & x_{i,4}(n) & x_{i,1}(n) & -x_{i,2}(n) \\ -x_{i,4}(n) & -x_{i,3}(n) & x_{i,2}(n) & x_{i,1}(n) \end{bmatrix}. \quad (36)$$

Due to the orthogonality of the code design, each frequency band contains full information about the transmitted symbols. As a result, the transmitted symbols are recovered perfectly when there is at least one unjammed frequency band.

In this case, the average probability of error P_e can be expressed as

$$P_e = \sum_{i=0}^4 P_{e,i} \Pr\{i \text{ out of 4 bands are jammed}\}, \quad (37)$$

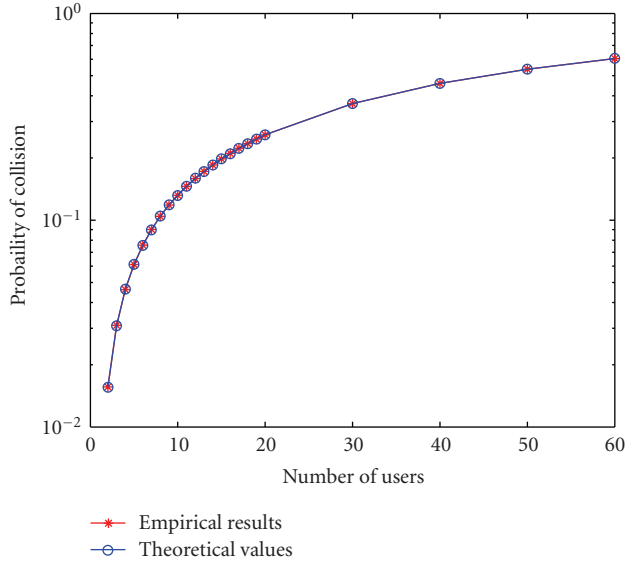


FIGURE 3: Probability of collision (P_h) versus the number of users (starting at the two-user case) for $N_c = 64$.

where $P_{e,i}$ is the probability of error when i out of 4 bands are jammed.

5.3. Spectral Efficiency. One major challenge in the current FH-OFDMA system is collision. In FH-OFDMA, multiple users hop their subcarrier frequencies independently. If two users transmit simultaneously in the same frequency band, a collision or hit occurs. In this case, the probability of bit error is generally assumed to be 0.5 [30].

If there are N_c available channels and M active users (i.e., $M - 1$ possible interfering users), all N_c channels are equally probable and all users are independent. Even if each user only transmit over a single carrier, then the probability that a collision occurs is given by

$$P_h = 1 - \left(1 - \frac{1}{N_c}\right)^{M-1} \quad (38)$$

$$\approx \frac{M-1}{N_c} \quad \text{when } N_c \text{ is large.}$$

Taking $N_c = 64$ as an example, the relationship between the probability of collision and the number of active users is shown in Figure 3. The high collision probability severely limits the number of users that can be simultaneously supported by an FH-OFDMA system.

In this example, $N_c = 64$, for a required BER of 0.04, only 6 users can be supported. That is, only 6 out of 64 subcarriers can be used simultaneously, and the carrier efficiency is $6/64 = 9.38\%$. On the other hand, due to the collision-free design, CFFH has the same spectral efficiency and BER performance as that of OFDM. For CFFH, the carrier efficiency is 100% with a much better BER performance. In this particular case, CFFH is approximately 10.67 times more efficient than the conventional FH-OFDMA system. This fact is further illustrated in Simulation Example 1 of Section 6.

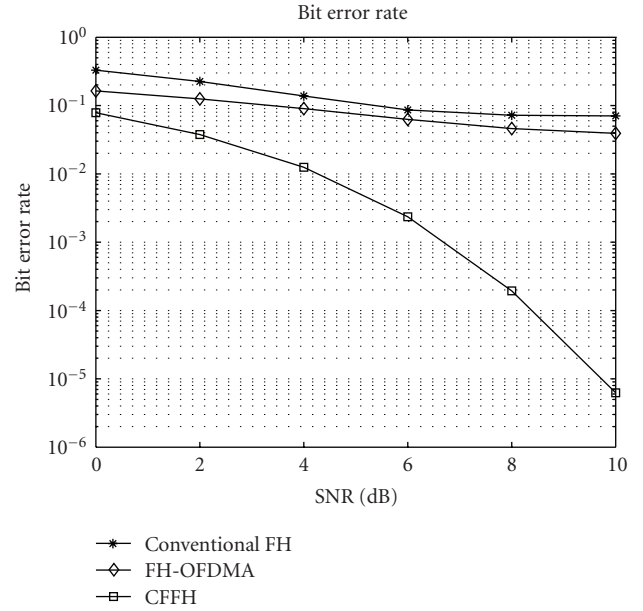


FIGURE 4: BER performance over AWGN channel of the CFFH, FH-OFDMA, and the conventional FH systems with $M = 8$ users and $N_c = 128$ available subcarriers.

6. Simulation Examples

In this section, we provide simulation examples to demonstrate the performance of the proposed schemes. First, the bit error performance of the proposed CFFH scheme, and the conventional FH and FH-OFDMA systems is performed under AWGN channels. Second, the bit error performance of the proposed CFFH and STC-CFFH schemes and the STC-OFDM system is performed over a frequency selective fading channel with partial-band jamming.

Simulation Example 1. We consider the conventional FH, the FH-OFDMA and the proposed CFFH systems, each with $M = 8$ users and $N_c = 128$ available subcarriers. The conventional FH system uses four-frequency shift keying (4-FSK) modulation, where each user transmits over a single carrier. Both the proposed CFFH and FH-OFDMA systems transmit 16-QAM symbols, and each user is assigned 16 subcarriers. The average bit error rate (BER) versus the signal-to-noise ratio (SNR) performance over AWGN channels of the systems is illustrated in Figure 4. As can be seen, the proposed CFFH scheme delivers excellent results since the multiuser access interference (MAI) is avoided. The conventional FH and FH-OFDMA schemes, on the other hand, are severely limited by collision effect among users.

Simulation Example 2. The BER performance of the STC-OFDM scheme and the proposed STC-CFFH and CFFH schemes is evaluated by simulations. The simulations are carried out over a frequency selective Rayleigh fading channel with partial-band jamming. A 2×2 Alamouti scheme is applied to the proposed STC-CFFH system. We assume perfect timing and frequency synchronization as well as uncorrelated channels for each antenna. The total number

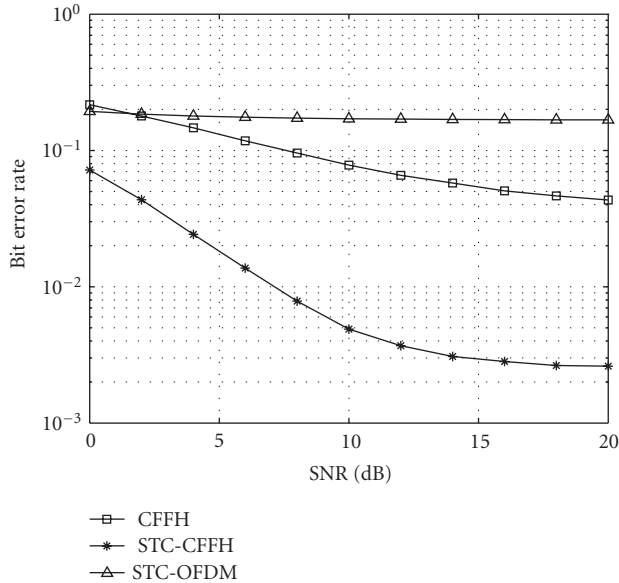


FIGURE 5: Comparison of the BER over frequency selective fading channel with partial-band jamming. Number of subcarriers $N_c = 256$, number of users = 16, and SJR = 0 dB.

of available subcarriers is $N_c = 256$, and the number of users is $M = 16$; therefore, each user is assigned 16 subcarriers.

We consider the performance of three systems that transmits 16-QAM symbols: (i) the proposed CFFH system; (ii) an STC-OFDM system, (iii) the proposed STC-CFFH system. For system (ii), each user transmits on 16 fixed subcarriers. In systems (i) and (iii), each user transmits on 16 pseudorandom secure subcarriers. We assume that the jammer intentionally interferes 16 subcarriers out of the whole band.

Figure 5 depicts the BER versus SNR over frequency selective fading with SJR = 0 dB. Due to secure subcarrier assignment, the proposed CFFH system outperforms the STC-OFDM system. The pseudorandom secure subcarrier assignment randomizes each users' subcarrier occupancy (i.e., spectrum occupancy) at a given time, therefore allowing for multiple access over a wide range of frequencies. Furthermore, incorporating space-time coding into CFFH significantly increases the BER performance. We also noticed that at high SNR levels, the performance limiting factor for all systems is the partial-band jamming. In Figure 6, the BER versus the jammer occupancy (ρ) is evaluated with SNR=10 dB and SJR=0 dB for the three systems. Recall that the jammer occupancy is the fraction of subcarriers that experience interference. We can see that the STC-CFFH system outperforms the other systems for all $\rho < 1$. This example shows that STC-CFFH is very robust under jamming interference.

We also observed that due to the randomness in the frequency hopping pattern as well as the fact that the system ensures collision-free transmission among the users, the performance of the proposed system remains the same as the number of users varies in the system.

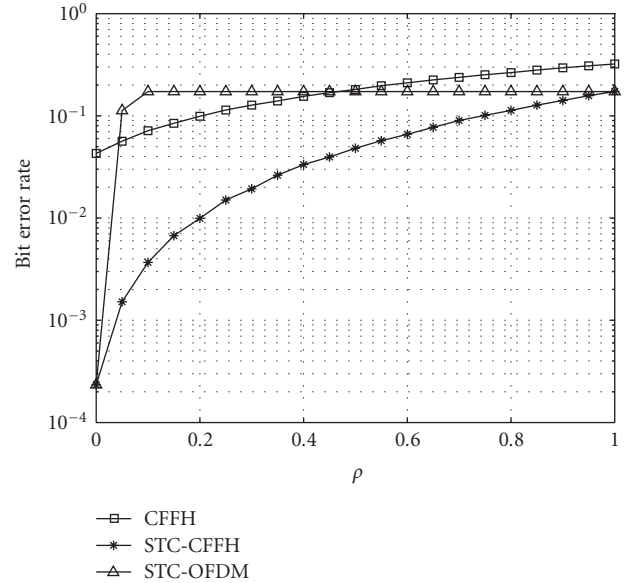


FIGURE 6: BER versus jammer occupancy over frequency selective fading channel with partial-band to full-band jamming. Number of subcarriers $N_c = 256$, number of users = 16, SJR = 0 dB, and SNR = 10 dB.

7. Conclusions

In this paper, we introduced a secure collision-free frequency hopping scheme. Based on the OFDMA framework and the secure subcarrier assignment algorithm, the proposed CFFH system can achieve high spectral efficiency through collision-free multiple access. While keeping the inherent antijamming and anti-interception security features of the FH system, CFFH can achieve the same spectral efficiency as that of OFDM and can relax the strict synchronization requirement suffered by the conventional FH systems. Furthermore, we enhanced the jamming resistance of the CFFH scheme by incorporating space-time coding to the proposed scheme. The OFDMA-based dynamic spectrum access control scheme proposed in this paper can be applied directly for secure and efficient spectrum sharing among different users and services in cognitive networks.

Acknowledgment

This work is partially supported by NSF under awards CNS-0746811 and CNS-0716039.

References

- [1] C. Martin, E. Lemois, F. Buda, and D. Merel, "Description of a complete multi-carrier spread spectrum transmission chain for robust and discrete tactical communications," in *Proceedings of the IEEE Military Communications Conference (MILCOM '00)*, vol. 2, pp. 942–946, October 2000.
- [2] J. Nilsson and T. Giles, "Wideband multi-carrier transmission for military HF communication," in *Proceedings of the IEEE Military Communications Conference (MILCOM '97)*, vol. 2, pp. 1046–1051, November 1997.

- [3] F. Dominique and J. H. Reed, "Robust frequency hop synchronisation algorithm," *Electronics Letters*, vol. 32, no. 16, pp. 1450–1451, 1996.
- [4] M. Simon, G. Huth, and A. Polydoros, "Differentially coherent detection of QASK for frequency-hopping systems—part I: performance in the presence of a gaussian noise environment," *IEEE Transactions on Communications*, vol. 30, pp. 158–164, 1982.
- [5] Y. M. Lam and P. H. Wittke, "Frequency-hopped spread-spectrum transmission with band-efficient modulations and simplified noncoherent sequence estimation," *IEEE Transactions on Communications*, vol. 38, no. 12, pp. 2184–2196, 1990.
- [6] J. Cho, Y. Kim, and K. Cheun, "A novel FHSS multiple-access network using M-ary orthogonal walsh modulation," in *Proceedings of the 52nd IEEE Vehicular Technology Conference*, vol. 3, pp. 1134–1141, September 2000.
- [7] S. Glisic, Z. Nikolic, N. Milosevic, and A. Pouttu, "Advanced frequency hopping modulation for spread spectrum WLAN," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 1, pp. 16–29, 2000.
- [8] K. Choi and K. Cheun, "Maximum throughput of FHSS multiple-access networks using MFSK modulation," *IEEE Transactions on Communications*, vol. 52, no. 3, pp. 426–434, 2004.
- [9] K.-C. Peng, C.-H. Huang, C. J. Li, and T. S. Horng, "High-performance frequency-hopping transmitters using two-point delta-sigma modulation," *IEEE Transactions on Microwave Theory and Techniques*, vol. 52, pp. 2529–2535, 2004.
- [10] K. Choi and K. Cheun, "Optimum parameters for maximum throughput of FHMA system with multilevel FSK," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 5, pp. 1485–1492, 2006.
- [11] C. Y. Wong, R. S. Cheng, K. B. Letaief, and R. D. Murch, "Multiuser OFDM with adaptive subcarrier, bit and power allocation," *IEEE Journal of Selective Areas on Communications*, 1999.
- [12] H. Sari, "Orthogonal frequency-division multiple access with frequency hopping and diversity," in *Multi-Carrier Spread Spectrum*, K. Fazel and G. P. Fettweis, Eds., Kluwer Academic Publishers, Norwell, Mass, USA, 1997.
- [13] US National Institute of Standards and Technology, "Federal information processing standards publication 197-announcing the ADVANCE ENCRYPTION STANDARD (AES)," 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [14] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, 1998.
- [15] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1456–1467, 1999.
- [16] V. Tarokh, H. Jafarkhani, and A. Calderbank, "Space-time codes for high data rate wireless communication: performance results," *IEEE Journal on Select Areas Communication*, pp. 451–460, 1999.
- [17] W. E. Burr, "Selecting the advance encryption standard," *IEEE Security and Privacy*, pp. 43–52, 2003.
- [18] J. Jang and K. B. Lee, "Transmit power adaptation for multiuser OFDM systems," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 2, pp. 171–178, 2003.
- [19] M. Ergen, S. Coleri, and P. Varaiya, "Qos aware adaptive resource allocation techniques for fair scheduling in OFDMA based broadband wireless access systems," in *Proceedings of the IEEE Transactions on Broadcasting*, vol. 49, pp. 362–370, December 2003.
- [20] S.-E. Elayoubi and B. Fourestie, "Performance evaluation of admission control and adaptive modulation in OFDMA WiMax systems," *IEEE/ACM Transactions on Networking*, vol. 16, no. 5, pp. 1200–1211, 2008.
- [21] K. F. Lee and D. B. Williams, "Space-frequency transmitter diversity technique for OFDM systems," in *Proceedings of the IEEE Global Telecommunications Conference*, vol. 3, pp. 1473–1477, November 2000.
- [22] B. Vucetic and J. Yuan, "Space time coding performance analysis and code design," in *Space Time Coding*, p. 2003, John Wiley & Sons.
- [23] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 744–765, 1998.
- [24] J. Park, D. Kim, C. Kang, and D. Hong, "Effect of partial band jamming on OFDM-based WLAN in 802.11g," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 560–563, April 2003.
- [25] P. J. Crepeau, "Performance of FH/BFSK with generalized fading in worst case partial-band gaussian interference," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 5, pp. 884–886, 1990.
- [26] M. B. Pursley and W. E. Stark, "Performance of reed-solomon coded frequency-hop spread-spectrum communications in partial-band interference," *IEEE Transactions on Communications*, vol. 33, no. 8, pp. 767–774, 1985.
- [27] W. E. Stark, "Coding for frequency-hopped spread-spectrum communication with partial-band interference—part II: coded performance," *IEEE Transactions on Communications*, vol. 33, pp. 1045–1057, 1985.
- [28] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread-spectrum communications—a tutorial," *IEEE Transactions on Communications*, vol. 30, no. 5, part 1, pp. 855–884, 1982.
- [29] C. E. Cook and H. S. Marsh, "Introduction to spread spectrum," *IEEE Communications Magazine*, vol. 21, no. 2, pp. 8–16, 1983.
- [30] T. S. Rappaport, *Wireless Communications*, Prentice-Hall, 2nd edition, 2002.