A Spectrally Efficient Frequency Hopping System

Tongtong Li   Qi Ling   Jian Ren
Department of Electrical & Computer Engineering
Michigan State University, East Lansing, Michigan 48824, USA.
e-mail:{tongli, lingqi, renjian}@egr.msu.edu

***Abstract*—Frequency hopping systems have been widely used in military communications to prevent hostile jamming, interception and detection. In traditional frequency hopping (FH) systems, the transmitter hops in a pseudo-random manner among available frequencies according to a pre-specified algorithm, and the receiver operates accordingly in exact synchronization with the transmitter's hopping pattern. In multiple access systems, a collision may happen when more than one users transmit in the same frequency band simultaneously. Two major limitations with the conventional frequency hopping systems are: strict requirement on frequency acquisition/synchronization, and very low spectral efficiency due to inefficient utilization of the available bandwidth. In this paper, we introduce a new concept — collision-free frequency hopping (CFFH). Based on the OFDM framework and the secure subcarrier assignment algorithm, the proposed CFFH system can achieve high information capacity through collision-free multiple access, and can successfully resolve the strict synchronization limitation. At the same time, as each user still transmits through a pseudo-random frequency hopping scheme, CFFH can maintain the inherent anti-jamming, anti-interception security features of the conventional FH system.**

I. INTRODUCTION

As one of the two basic modulation techniques used in spread spectrum communications [1], frequency hopping technique was originally designed to be inherently secure and reliable under adverse battle conditions for military purpose. In a conventional FH system, the transmitter "hops" in a pseudo-random manner among available frequencies according to a pre-specified algorithm, the receiver then operates in synchronization with the transmitter and remains tuned to the same center frequency. Since it is unlikely that different bands experience simultaneous fading, FH systems are robust against fast fading. At the same time, the pseudo-random hopping of frequencies during radio transmission minimizes the possibility of hostile jamming and unauthorized interception.

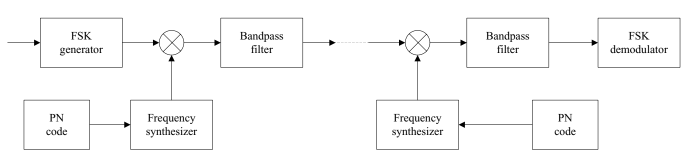

Fig. 1. The block diagram of the conventional frequency hopping scheme

In 1978, Cooper and Nettleton [2] first proposed a frequency hopping multiple access (FHMA) system with differential phase shift-keyed (DPSK) signaling for mobile communication applications. Later in the same year, Viterbi [3] initiated the use of MFSK for low-rate multiple access mobile satellite systems. Since it enables non-coherent detection, MFSK modulation has been widely adopted in FHMA systems [4]–[7].

To improve the information capacity of FHMA systems, considerable efforts have been devoted to applying high-dimensional modulation schemes to the FH systems [8], [9]. However, limited by the collision effect, the spectral efficiency of existing frequency hopping systems is still very low due to inefficient use of the large bandwidth. Along with development on high rate wireless multimedia communications, there has been an ever increasing demand on transmitting more information without extra bandwidth. At the same time, in today's FH systems, strict synchronization requirement is another major issue. The frequency hopping rate is mainly determined by the frequency agility of receiver synthesizers. Therefore, new system design ideas need to be introduced to overcome these two shortcomings (i.e, low spectral efficiency and stringent synchronization requirement) in existing FH systems.

In this paper, we propose a highly bandwidth-efficient collision-free frequency hopping (CFFH) scheme. The new system is based on the OFDM (orthogonal frequency division multiplexing) framework. At each hopping period, each user transmits on specific subcarrier(s), based on the user's information rate requirement and total load of the system. An AES (advanced encryption standard) based secure subcarrier assignment algorithm is proposed to ensure that: (i) Each user hops to a different set of subcarriers in a pseudo-random manner at the beginning of each hopping period; (ii) At each hopping period, different users always transmit on non-overlapping sets of subcarriers, and hence are collision-free.

The major features of the proposed CFFH scheme can be summarized as follows. First, since the new system utilizes the OFDM modulation, which is implemented through FFT (Fast Fourier Transform), CFFH relaxes the complex frequency synchronization problem suffered by conventional FH systems. Second, CFFH is highly spectrally efficient because it is collision-free and makes full use of the available spectrum. The spectral efficiency of the proposed CFFH scheme is also enhanced by the OFDM framework. OFDM allows frequency overlapping between subcarriers which are orthogonal to each other, and hence is much more efficient than the conventional

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

FH system where guard band is needed between neighboring channels. Third, ensured by AES, CFFH maintains the inherent anti-jamming and anti-interception security feature of conventional FH systems. Furthermore, in multiple access environment (which can be achieved by sending dummy bits on certain subcarriers), anonymous multiparty communication can be achieved and hence can prevent traffic analysis by the hostile party. We would like to emphasize that while it is possible to design collision-free frequency hopping system based on non-OFDM frameworks, the utilization of OFDM in the CFFH scheme has unique advantages which can not be surpassed by other systems.

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

The core components of the CFFH system is the OFDM system and the secure subcarrier assignment algorithm. Here we first describe the signal transmission scheme for each individual user, then present the AES based dynamic subcarrier assignment algorithm. *For notation simplification, here we assume that the hopping period equals one OFDM symbol period, but the results can be directly extended to more general cases.*

A. Signal Transmission and Detection

Consider a system with M users, utilizing an OFDM system with N subcarriers, $\{f_0, \cdots, f_{N-1}\}$. At each OFDM symbol period, each user is assigned a specific subset of the total available subcarriers. Assuming that at the nth symbol, user i has been assigned a set of sub-carriers $C_{n,i} = \{f_{n,i_1}, \cdots, f_{n,i_{N_i}}\}$, that is, user i will transmit and only transmit on these subcarriers. Here N_i is the total number of subcarrier assigned to user i. Note that for any n,

$$C_{n,i} \bigcap C_{n,j} = \emptyset, \quad \text{if} \quad i \neq j. \tag{1}$$

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,

$$\bigcup_{i=1}^{M} C_{n,i} = \{f_1, \cdots, f_N\}. \tag{2}$$

For the ith user, if $N_i > 1$, then the ith users information symbols are first fed into a serial-to-parallel converter. Assuming that at the nth symbol period, user i transmits the information symbols $\{u_{n,1}^{(i)}, \cdots, u_{n,N_i}^{(i)}\}$ (which are generally QAM symbols) through the subcarrier set $C_{n,i} = \{f_{n,i_1}, \cdots, f_{n,i_{N_i}}\}$. User i's transmitted signal at the nth OFDM symbol can then be written as:

$$s_n^{(i)}(t) = \sum_{l=1}^{N_i} u_{n,l}^{(i)} e^{j2\pi f_{n,i_l} t}. \tag{3}$$

Note that each user transmits zeros on subcarriers which are not assigned to him/her, and hence ensures collision-free transmission among the users.

At the receiver, the received signal is a superposition of the signals transmitted from all users

$$r(t) = \sum_{i=1}^{M} r_n^{(i)}(t) + n(t), \tag{4}$$

where

$$r_n^{(i)}(t) = s_n^{(i)}(t) * h_i(t), \tag{5}$$

and $n(t)$ is the additive noise. In (5), $h_i(t)$ is the channel impulse response corresponding to user i. Note that in OFDM systems, guard intervals are inserted between symbols to eliminate intersymbol interference, so it is reasonable to study the signals in a symbol-by-symbol manner. Equations (3)-(5) represent an uplink system. The downlink system can be formulated in a similar manner.

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

$$\mathbf{u}_n^{(i)}(l) = \begin{cases} 0, & l \notin \{i_1, \cdots, i_{N_i}\} \\ u_{n,l}^{(i)}, & l \in \{i_1, \cdots, i_{N_i}\}. \end{cases} \tag{6}$$

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

$$\mathbf{s}_n^{(i)} = \mathbf{F}\mathbf{u}_n^{(i)}, \tag{7}$$

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

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

with $W_N^{nk} = e^{j2\pi nk/N}$. 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 intersymbol interference between two successive OFDM symbols).

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

$$\mathbf{H}_i = \mathbf{F}^{\mathbf{H}}\mathbf{h}_i \tag{8}$$

be the Fourier transform of $\mathbf{h}_i$, where $(\cdot)^H$ denote the Hermitian transpose. Then after FFT, the received signal corresponding to user i is

$$\mathbf{r}_n^{(i)}(l) = \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l). \tag{9}$$

The overall received signal is then given by

$$\mathbf{r}_n(l) = \sum_{i=1}^{M} \mathbf{r}_n^{(i)}(l) + \mathbf{N}_n(l) \tag{10}$$

$$= \sum_{i=1}^{M} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l) + \mathbf{N}_n(l). \tag{11}$$

1930-529X/07/$25.00 © 2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

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

Note that due to the collision-free subcarrier assignment, for each l, there is at most one non-zero item in the sum $\sum_{i=1}^{M} \mathbf{u}_n^{(i)}(l)\mathbf{H}_i(l)$. As a result, standard channel estimation algorithms and signal detection algorithms for OFDM systems can be implemented.

In the slow hopping case, where each user transmits a frame of OFDM symbols before it hops to a different set of subcarrier, 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 need to estimate the entries corresponding to its subcarrier set, that is the values of $\mathbf{H}_i(l)$ for $l \in \{i_1, \cdots, i_{N_i}\}$. After channel estimation, user i's information symbols can be estimated from

$$\mathbf{u}_n^{(i)}(l) = \frac{\mathbf{r}_n^{(i)}(l)}{\mathbf{H}_i(l)}, \quad l \in \{i_1, \cdots, i_{N_i}\}. \tag{12}$$

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.

In the fast hopping case, where the hopping period is less than or equal to one OFDM period, each user would then send one to two pilot (full OFDM) symbols, so that the channel information is available no matter which subcarrier set the user hops to. When there are multiple users in the system, different users should transmit their pilot symbols in non-overlapping time periods for accurate channel estimation.

B. The Secure Subcarrier Assignment Algorithm

Design of the secure subcarrier assignment algorithm is not unique, here we present an AES (Advanced Encryption Standard) based secure carrier index assignment algorithm. The AES algorithm is used here to ensure the security of the hopping system, so that it is extremely difficult for the malicious users to find out the hopping pattern. Certainly, other advanced encryption algorithms can be implemented here as well.

Without loss of generality, here we assume that the total number of carriers $N = 128$. The following algorithm can be extended directly to other values of N. The proposed secure subcarrier assignment algorithm can be summarized as follows:

1) Generate a pseudo-random binary sequence using a 42-bit linear feedback shift register (LFSR) specified by the following characteristic polynomial:

$$\begin{aligned} &x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} \\ &+x^{22} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} \\ &+x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1, \end{aligned} \tag{13}$$

Group the sequence into blocks of length 128 bits, denote the nth block as $\mathbf{X}_n$, which will be used to generate the subcarrier index for the nth OFDM symbol.

2) Take the nth block $\mathbf{X}_n$ as the plaintext, and specify a 128-bit key. Encrypt the plaintext with the key using the AES algorithm, and the length of the ciphertext is also 128 bits, denoted by $\{pc_0,\ pc_1,\ \cdots,\ pc_{127}\}$.

3) Because the subcarrier index is from 0 to 127, each position can be represented by $\log_2(128) = 7$ bits. Form a 1×134 vector by cyclic padding, $[pc_0\ pc_1\ \cdots\ pc_{127}\ pc_0\ pc_1\ \cdots\ pc_5]$. Then divide it into 128 7-bit groups:

$$\begin{aligned} &[pc_0\ pc_1\ \cdots\ pc_6],\ [pc_1\ pc_2\ \cdots\ pc_7] \\ &\cdots,\ [pc_{127}\ pc_0\ \cdots\ pc_5]. \end{aligned} \tag{14}$$

4) For $i = 0, 2, \cdots, 127$, let $P(i)$ denote the decimal number corresponding to the ith 7-bit vector, $[pc_{(i-1)}\ pc_{(i\ mod\ 128)}\ \cdots\ pc_{(i+5\ mod\ 128)}]$, i.e.,

$$\begin{aligned} P(i) &= pc_{i-1} \cdot 2^6 && +pc_{(i\ mod\ 128)} \cdot 2^5 \\ &+ pc_{(i+1\ mod\ 128)} \cdot 2^4 && +pc_{(i+2\ mod\ 128)} \cdot 2^3 \\ &+ pc_{(i+3\ mod\ 128)} \cdot 2^2 && +pc_{(i+4\ mod\ 128)} \cdot 2^1 \\ &+ pc_{(i+5\ mod\ 128)} \cdot 2^0 && . \end{aligned}$$

Define $\mathcal{P} = [P(1)\ P(2)\ \cdots\ P(128)]$. $\mathcal{P}$ does not necessarily contain all the numbers from 1 to 128 as there might appear repeated numbers. The following operations aim to replace all the repeated numbers with the missing numbers:

a) Stack all the missing numbers in $\mathcal{P}$ from $[0, 1, 2, \cdots, 127]$ into a vector $\mathcal{A}$, $\mathcal{A} = [A(1)\ A(2)\ \cdots\ A(\mathcal{M})]$.

b) Find the index of each repeated number in $\mathcal{P}$ and stack them to formulate a vector $\mathcal{B}$, $\mathcal{B} = [B(1)\ B(2)\ \cdots\ B(\mathcal{M})]$. Clearly the length of $\mathcal{A}$ is equal to that of $\mathcal{B}$.

c) Let $\mathcal{P}(B(i)) = A(i)$, i.e., substitute $A(i)$ for the $B(i)$'s entry in $\mathcal{P}$.

The update vector $\mathcal{P}$ contains all the numbers from 0 to 127, and each number occurs only once.

5) Recall that at each OFDM symbol, N_i subcarriers is assigned to user i. We now assign the subcarriers with indexes $\{P(0), P(1), \cdots, P(N_1 - 1)\}$ to user 1, assign the subcarriers with indexes $\{P(N_1), \cdots, P(N_1 + N_2 - 1)\}$ to user 2, and so on.

III. Performance Analysis

One major challenge in the current frequency hopping multiple access (FHMA) system is collision. In FHMA systems, multiple users hop their carrier 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.

If there are N available channels and M active users (i.e., $M - 1$ possible interfering users), assuming all N channels are equally probable and all users are independent, then the probability that a collision occurs is given by

$$P_h = 1 - (1 - \frac{1}{N})^{M-1} \approx \frac{M-1}{N} \quad \text{when } N \text{ is large.} \qquad (15)$$

Taking $N = 64$ as an example, the relationship between the probability of collision and the number of active users is shown

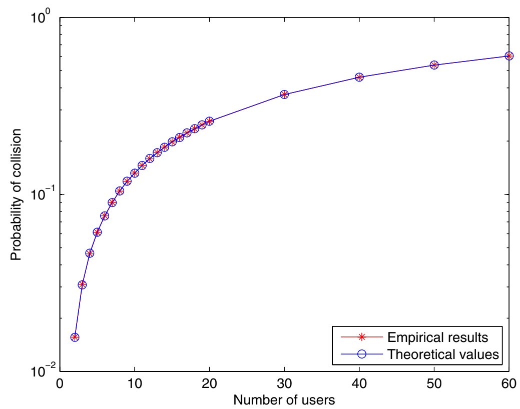

Fig. 2. Probability of collision (P_h) versus the number of users (starting at the 2-user case) for $N = 64$.

in Fig. 2. The high collision probability severely limits the number of users that can be simultaneously supported by an FH system. If $P_{e,M}$ is the probability of bit error for the modulation scheme used in the single user case, the overall probability of bit error in the exiting FHMA system is given by

$$P_e = P_{e,M}(1 - P_h) + \frac{1}{2}P_h. \qquad (16)$$

Assuming BFSK modulation and $N_h = 1$ (here N_h is the number of hops per symbol period), for example, the probability of bit error can be modeled as $P_e = \frac{1}{2}e^{-\frac{E_b}{2N_o}}(1 - P_h) + \frac{1}{2}P_h$, where $\frac{E_b}{N_o}$ is the bit level signal-to-noise ratio (SNR).

Simulation Example 1 — BER performance and Spectral Efficiency Assume that total number of available channels (carriers) is $N = 128$. Consider two systems: (i) A conventional FHMA system with $M = 8$ users, each using 4-FSK modulation; (ii) A CFFH system with 8 users, each transmitting QPSK symbols. The BER comparison of the two systems over AWGN channels is shown in Figure. 3. As can be seen, the proposed CFFH system delivers excellent results. The conventional FHMA system, on the other hand, is severely limited by the collision effect, and does not really work. And it should be note that in this example, the the spectral efficiency of the CFFH system is 16 times that of the conventional FHMA system. Essentially, CFFH has the same spectral efficiency as the OFDM system, which is much higher than the conventional FHMA system.

Simulation Example 2 — Jamming Resistance In this example, the total number of available subcarriers is $N = 256$ and the number of users is $M = 16$. Each user is assigned 16 subcarriers. Consider the performance of three systems under hostile jamming: (i) A conventional OFDMA system where each user transmits on 16 fixed subcarriers; (ii) A CFFH system with 16 subcarriers allocated to each user pseudo-randomly based on the secure subcarrier assignment. (iii) A CFFH system with the knowledge of which subcarriers being jammed, where users are able to choose channels for information transmission to avoid the hostile jamming. This case is essentially equivalent to a jamming-free CFFH or OFDMA system. We assume that the jammer intentionally interferes 8 subcarriers, which are coincidentally used by the user in system (i). E_b/P_J is defined as the ratio of the average bit-level energy to the total jamming power. SNR is defined as the ratio of the average signal power to the noise power, and is fixed at 7 dB in the simulation.

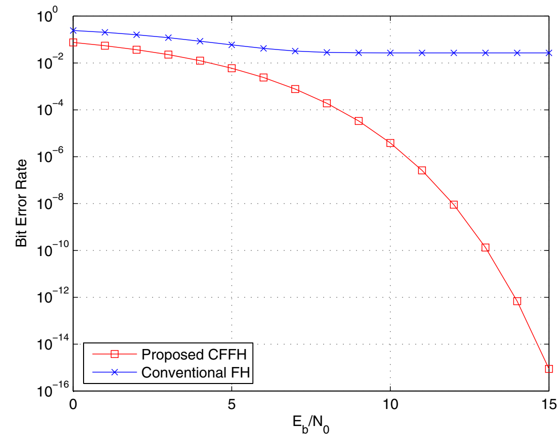

Fig. 3. Comparison of the BER over AMGN channels. Number of channels $N = 128$, number of users = 8, and the spectral efficiency of the CFFH system is 16 times that of the conventional FHMA system.

At the transmitter, a rate-$\frac{1}{2}$ turbo encoder is utilized for forward error control. The generation matrix of the constituent code is given by $[1, \frac{(7)_{octal}}{(5)_{octal}}]$, where $(7)_{octal}$ and $(5)_{octal}$ are the feedback and feedforward polynomials with memory length 2, respectively. The block length is 960. After encoding, 1920 bits are mapped into 16-QAM symbols and transmitted over the selected carriers. At the receiver, tentative hard decisions are made on the outputs of 16-QAM demodulation, and there is no iteration between the demodulator and the turbo decoder. The decoding algorithm is the canonical log-MAP. The number of decoding iterations is 5, and no early termination scheme is applied.

The BER comparison of the three systems over the same AWGN channel is shown in Fig. 4. As can be seen, benefited from the jamming resistance property of the frequency hopping system, the proposed CFFH delivers much better performance under hostile jamming than that the conventional OFDMA system with fixed carrier allocation. The performance of the conventional OFDMA system is severely limited by the jamming interference, even if a powerful error-correcting code (e.g., turbo coding) is employed. System (iii) is essentially jamming-free and its BER performance serves as the lower bound in this example.

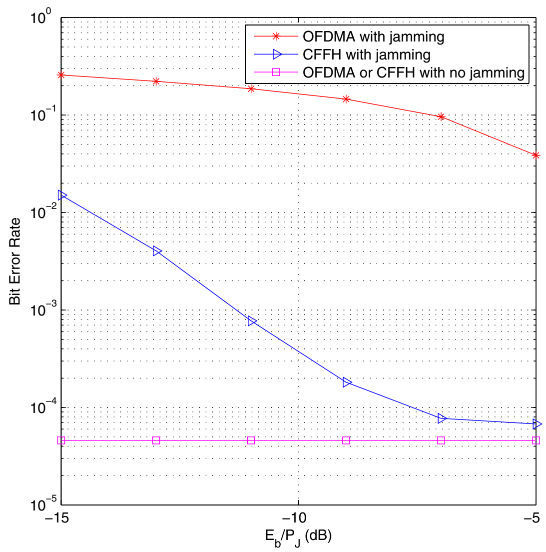

Fig. 4. BER comparison of the three systems, SNR = 7dB.

IV. Conclusions

In this paper, we introduced a highly efficient secure communication interface — the collision-free frequency hopping (CFFH) system. Based on the OFDM framework and the secure subcarrier index assignment algorithm, the proposed CFFH system can achieve high spectral efficiency through collision-free multiple access. While keeping the inherent anti-jamming, anti-interception security features of the FH system, CFFH resolved the strict synchronization requirement suffered by the conventional FH systems. Our simulation experiments demonstrated the superior performance of the CFFH scheme in terms of both spectral efficiency and jamming resistance.

References

[1] T. S. Rappaport, *Wireless Communications - Principles and Practices*, 2nd ed. Prentice Hall, 2002.

[2] G. Cooper and R. Nettleton, "A spread spectrum technique for high capacity mobile communuzation," *IEEE Trans. Veh. Technol.*, vol. 27, pp. 264–275, Nov 1978.

[3] A. Viterbi, "A processing-satellite transponder for multlple access by low rate mobile users," in *Proc. Digital Satellite Commun. Conf.*, Montreal, Canada, Oct 1978.

[4] E. Geraniotis, "Multiple-access capability of frequency-hopped spread-spectrum revisited: An analysis of the effect of unequal power levels," *IEEE Trans. Commun.*, vol. 38, pp. 1066–1077, Jul 1990.

[5] Y. Tsai and J. Chang, "Using frequency hopping spread spectrum technique to combat multipath interference in a multiaccessing environment," *IEEE Trans. Veh. Technol.*, vol. 43, pp. 211–222, May 1994.

[6] M. Wickert and R. Turcotte, "Probability of error analysis for FHSS/CDMA communications in the presence of fading," *IEEE J. Sel. Areas Commun.*, vol. 10, pp. 523–534, Apr 1992.

[7] E. Geraniotis and M. Pursley, "Error probabilities for slow frequency-hopped spread-spectrum multiple-access communication over fading channels," *IEEE Trans. Commun.*, vol. 30, pp. 996–1009, May 1982.

[8] K. Choi and K. Cheun, "Maximum throughput of fhss multiple-access networks using MFSK modulation," *IEEE Trans. Commun.*, vol. 52, pp. 426–434, Mar 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 Trans. Microw. Theory Tech.*, vol. 52, pp. 2529–2535, Nov 2004.