Secure Spectrum-Efficient Frequency Hopping for Return Link of Protected Tactical Satellite Communications

Lun Li, Xin Tian, Genshe Chen
Intelligent Fusion Technology, Inc.
Germantown, MD 20876
{lun.li,xtian,gchen}@intfusiontech.com

Khanh Pham
Air Force Research Lab
Kirtland AFB, NM 87117
khanh.pham.1@us.af.mil

Erik Blasch
Air Force Research Lab
Rome, NY 13441
erik.blasch.1@us.af.mil

***Abstract*—Protected tactical waveform (PTW) provides cost-efficient, jamming-resistant communications via both government and commercial satellites over multiple frequency bands such as the C-, Ku-, Ka-, and X-band. Frequency hopping (FH) was originally developed for secure communications by exploiting time-frequency diversity over a large spectrum. The anti-jamming feature of the frequency hopping technique helps communication systems improve the reliability of transmission. In this paper, we consider a secure channel group hopping (CGH) scheme in order to satisfy the needs of protected tactical satellite communication system. This scheme is proposed to ensure that each channel group hops to a new hopping spectrum in a pseudo-random manner during each hopping period, and different channel groups always transmit over non-overlapping frequency bands. Our analysis suggests that the proposed CGH scheme achieves collision-free frequency hopping among channel groups, such that a higher spectrum efficiency of the system can be obtained. Simulation results are provided to validate the performance of the proposed CGH scheme for PTW system.**

I. Introduction

In wireless communication networks, one of the most commonly used techniques to degradate the communication quality of opponent's signals is referred to jamming [1], which is that the adversary deliberately interferes the authorized users by sending malicious signals. Currently, along with the development of cognitive radios [2], [3], [4], jamming attacks are not only limited to secured communications [5], but also produce a serious negative effect in commercial communications [6]. Many communication applications such as symbol detection [7], [8], image transmission [9], and communication scheduling [10], [11] can be significantly degraded by jamming attacks. In the past decades, various anti-jamming techniques have been developed to secure wireless communication systems from malicious attacks.

Frequency hopping (FH) [12], [13], [14] is a technique that spreads its signal over rapidly changing frequencies, which was originally designed for jamming resistant communications. In traditional FH communication systems, the transmitter hops signals among available frequencies within a pre-specified hopping spectrum in a pseudo-random manner. The receiver then operates the received signals in a strict synchronization with the transmitter. FH has been widely applied in wireless networks due to its distinguished anti-jamming capability. In current communication systems, multiple users are usually supported, such that frequency hopping multiple access (FHMA) [15], [16] methodology has been developed, which is a spread-spectrum (SS) transmission technology that lets various users concurrently occupy the exact the same hopping spectrum. In SS FHMA, every user stays at a certain narrowband channel at a specific hopping period, depending on the users unique pseudo-random number (PN) sequence. However, in conventional FHMA, each user hops its signals independently based on its own PN sequence. A collision occurs when there are two users hopping their signals into the same frequency band. The collision effect leads to the very low spectral efficiency of the conventional FHMA.

Protected tactical waveform (PTW) aims to support secure tactical systems in order to provide low-cost, high-reliability wireless communications. The PTW is developed with frequency hopping spread spectrum to support a higher anti-jamming capability by using both protected government and commercial frequency bands. The PTW has several features which are related to the topic of this paper. It includes that (i) PTW supports multiple users to transmit over the system through transmission security (TRANSEC); (ii) PTW supports FH, and achieves a distinguished anti-jamming capability; and (iii) PTW also utilizes the waveform of commercial satellite communication standard: Digital Video Broadcasting Satellite Second generation (DVB-S2) [17], [18] and Digital Video Broadcasting Return Channel via satellite (DVB-RCS).

Based on the requirements of a PTW system and drawbacks of conventional FHMA, and inspired by the frequency hopping scheme in [19], [20], [21], this paper focuses on developing an efficient frequency hopping scheme that supports multiple users simultaneously while preventing collision. We propose a secure channel group assignment scheme that is achieved by using advanced encryption standard (AES) based permutation algorithm. This scheme ensures that (i) each channel group hops to a new hopping spectrum in a pseudo-random manner in each hopping period; (ii) different channel groups always occupy non-overlapped frequency bands, such that the collision can be avoided; (iii) the return link hopping channel groups can have a different bandwidth, and each channel group is assigned by continuous frequency bands; and (iv)

978-1-5090-3781-6/16/$31.00 ©2016 IEEE

Fig. 1. Return Link Multi-access Architecture

the authorized users are able to avoid jamming attacks since malicious users cannot determine the hopping pattern.

The rest of this paper is organized as follows. Section II overviews the system background and introduces the terminology used in the paper. Section III presents the AES-based channel group assignment scheme. Section IV analyzes the spectral efficiency of the proposed channel group hopping. Section V provides the simulation results. Finally, Section VI concludes the paper.

II. System Overview

The multi-access structure of the PTW system return link is illustrated in Fig. 1. Based on the mission plan, the return link channels with different bandwidths are grouped into channel groups. It is observed from Fig. 1, channel groups can be of various bandwidths interoperating with a different number of channels with a different bandwidth. For return link frequency hopping, channel groups hop over available hopping spectrum. Note that the channels that are grouped together remain in the same channel group in the hopping process.

Multiple users may share one channel group, and each user receives a channel assignment file from system controller. However, the channel assignment scheme for users that hop in the same channel group is not in the scope of this paper. In this paper, we only consider a secure channel group assignment scheme over hopping spectrum to ensure a collision-free return link frequency hopping.

III. Secure Channel Group Assignment

In this section, we propose a secure channel group assignment scheme, which consists of three major steps including (i) PN sequence generation; (ii) AES encryption; and (iii) channel group index permutation.

By using a secure assignment scheme, the frequency hopping pattern is generated for each channel group so that channel groups are securely assigned a partition of the hopping spectrum, and hop on non-overlapping spectrum frequencies in each hopping period.

For the analysis, it is assumed that there is N_c available channel groups with different bandwidth $\{B_0, B_1, ...B_{N_c-1}\}$ pre-assigned by mission plan. The total available hopping spectrum is B, and different channel groups transmit on non-overlapping portions of available spectrum, so we have $\sum_{i=0}^{N_c-1} B_i = B$. The secure channel group hopping (CGH) scheme is described in the following subsections.

A. PN Sequence Generation

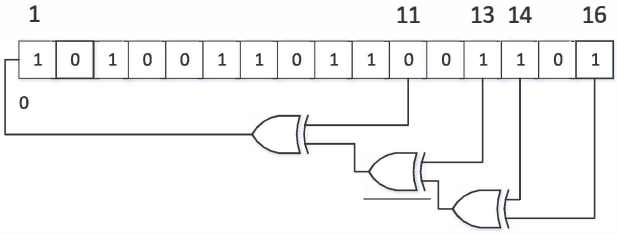

Fig. 2. 16-bit LFSR Structure

A 16-bit linear feedback shift register (LFSR) [22] whose input bit is a linear function of previous state is used to generate a pseudorandom binary sequence. In this design, the linear function used in LFSR is exclusive-or (XOR). The initial secret sequence is chosen by the system controller, and since the operation of LFSR is deterministic, then the output values of register is only determined by its previous state. Since the LFSR has a finite state, then the sequence starts repeating again. However, an LFSR with a well-chosen linear function

can generate a pseudorandom sequence with a long circle. The characteristic polynomial of the LFSR is written as

$$x^{16} + x^{14} + x^{13} + x^{11} + 1 \quad (1)$$

and the structure of the applied LFSR is shown in Fig. 2. The bit positions that affect the next state are called *taps*. The taps of applied LFSR from Fig. 2 are $\{16, 14, 13, 11\}$. The rightmost bit is called output bit, and the tap bits are sequentially combined with the output bit passing through XOR gate then fed back to the leftmost bit. The leftmost bits constitute the output pseudorandom sequence. Here, the register cycles sequences with the length of $2^{16} - 1 = 65535$ pseudorandom numbers, since the all zero state is excluded. Note that more sophisticated LFSR with complex structure can be applied in order to generate PN sequence with a longer circle, however in this paper, a 16-bit LFSR is considered for simplicity.

B. AES Encryption

In this subsection, a PN sequence generated by LFSR is used as plaintext. The plaintext is encrypted by AES algorithm [23] and a secure key. AES is designed based on a substitution-permutation network (SPN), which is illustrated in Fig. 3 In cryptography, SPN uses block cipher algorithm by taking a block of plaintext and the key as inputs, and adopts several rounds or layers of substitution boxes (S_i in Fig. 3, $i = 1, ..., 4$) and permutation boxes (P in Fig. 3) to generate the ciphertext. AES has a fixed block size of 128 bits, and the key size can be 128, 192, or 256 bits depending on the number of repetitions of rounds that AES ciphers the plaintext into ciphertext.

N_c is assumed to be a power of 2 for simple demonstration, and arbitrarily picks an integer $L \in [N_c/2, N_c]$. Note that L determines the number of channel group index permutation steps. $N_s = log_2 N_c$ bits represent each portion of the total spectrum B to be assigned to N_c channel groups. Let $b = LN_s$. We form a b-bit sequence $\mathbf{c} = [c_1, c_2, ..., c_b]$ by taking b bits from the ciphertext.

C. Secure Channel Group Index Permutation and Assignment

To enhance group analysis, the ciphertext sequence $\mathbf{c}$ is divided into L groups, such that each group has N_s bits. For $k = 1, 2, ...L$, the partition of the ciphertext sequence is described as follows.

$$\mathbf{p}_k = \{c_{[(k-1)*N_s+1)]}, c_{[(k-1)*N_s+2)]}, \cdots, c_{[(k-1)*N_s+N_s)]}\} \quad (2)$$

where $\mathbf{p}_k$ denotes the kth partition of ciphertext sequence in bits.

The decimal number P_k which corresponds to $\mathbf{p}_k$ can be calculated to formulate the permutation index vector. For $k = 1, 2, ...L$, then

$$\begin{aligned} P_k =& \sum_{i=1}^{N_s} \mathbf{p}_k(i) \cdot 2^{N_s - i} \\ =& c_{[(k-1)*N_s+1)]} \cdot 2^{N_s-1} + c_{[(k-1)*N_s+2)]} \cdot 2^{N_s-2} \\ &+ ... + c_{[(k-1)*N_s+N_s)]} \cdot 2^0 \end{aligned} \quad (3)$$

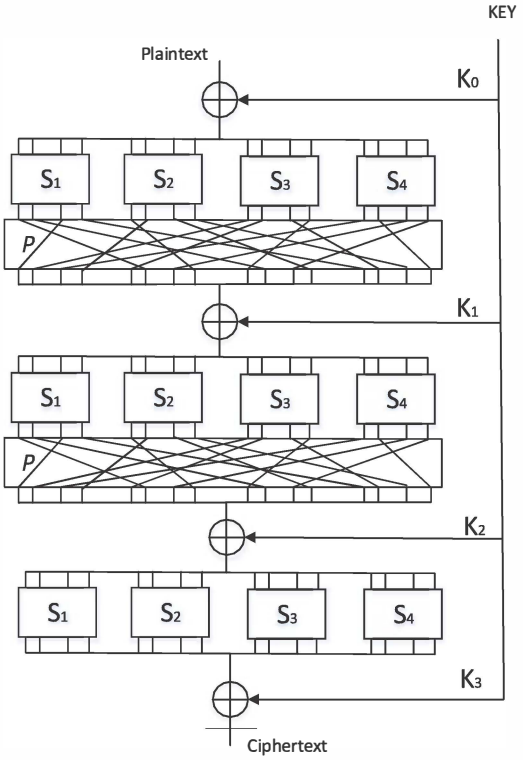

Fig. 3. Substitution-permutation Network

With each element P_k calculated, the permutation index vector is $\mathbf{P} = [P_1, P_2, ..., P_L]$, and decimal numbers in $\mathbf{P}$ ranges from 0 to $N_s - 1$. Now, denote the index vector at kth step $\mathbf{I}_k = [I_k(0), I_k(1), ..., I_k(N_c - 1)]$, $k = 0, 1, ..., L$. The permutation index scheme is determined by the following steps.

Step 0. Initialization: initialize the index vector $\mathbf{I}_0$ by giving any arbitrary permutation ranging from 0 to $N_c - 1$. Start with $\mathbf{I}_0 = [0, 1, ..., N_c - 1]$ for simple demonstration.

Step 1. Update: when $k = 1$, switch $I_0(0)$ and $I_0(P_1)$ within the index vector $\mathbf{I}_0$ to obtain $\mathbf{I}_1$, such that $\mathbf{I}_1 = [I_1(0), I_1(1), ..., I_1(N_c - 1)]$, where $I_1(n) = I_0(n)$ for $n \neq 0, P_1$, $I_1(0) = I_0(P_1)$, and $I_1(P_1) = I_0(0)$. Generalize the following steps by repeating the previous step for $k = 2, 3, ..., L$ to obtain $\mathbf{I}_k[I_k(0), I_k(1), ..., I_k(N_c - 1)]$ with the knowledge of its previous index vector $\mathbf{I}_{k-1} = [I_{k-1}(0), I_{k-1}(1), ..., I_{k-1}(N_c - 1)]$ by switching $I_k(k-1) = I_{k-1}(P_k)$, $I_k(P_k) = I_{k-1}(k-1)$, and maintaining $I_k(n) = I_{k-1}(n)$ for $n \neq k-1, P_k$.

Step 2. Stop: denote the initial channel group frequency vector as $\mathbf{f}_0 = [f_0, f_0, ..., f_{N_c-1}]$, where $f_{m+1} = f_m + B_m$, $m = 0, ..., N_c - 2$. After updating L steps, the channel group index vector as $\mathbf{I}_L = [I_L(0), I_L(1), ..., I_L(N_c - 1)]$, obtains the channel group frequency vector as $\mathbf{f}_L = [f_{I_L(0)}, f_{I_L(1)}, ..., f_{I_L(N_c-1)}]$. kth element in $\mathbf{f}_L$ is assigned to kth channel group ($k = 1, 2, ..., N_c$) as the lower frequency position.

Proposition 1: The proposed channel group assignment scheme ensures different channel groups transmit on different portions of hopping spectrum in each hopping period.

Proof: The channel group frequency vector is $\mathbf{f}_L = [f_{I_L(0)}, f_{I_L(1)}, ..., f_{I_L(N_c-1)}]$ after L steps of index permutation. Since $\mathbf{I}_L = [I_L(0), I_L(1), ..., I_L(N_c-1)]$ are nothing but obtained from the initial index vector $\mathbf{I}_0 = [0, 1, ..., N_c - 1]$ by switching the positions of the elements according to the permutation vector $\mathbf{P} = [P_1, P_2, ..., P_L]$, each index appears in $\mathbf{I}_L$ once and only once, such that N_c channel groups are assigned with the order of the indexes in $\mathbf{I}_L$ over the hopping spectrum. As a result, the channel group assignment scheme ensures that (i) all channel groups transmit on non-overlapping frequency bands over the hopping spectrum; and (ii) no idle band is in the hopping spectrum which means that all frequency bands are active for transmission in each hopping period. Note that if the secure channel group assignment scheme is operated in system controller, then the system controller encrypts the information of assignment and sends the hopping pattern periodically to each channel group.

IV. Spectral Efficiency Analysis

In this section, we analyze the spectral efficiency of the proposed channel group assignment scheme. As explained in Section I, collision has been challenging for conventional FHMA schemes in which multiple channel groups hop independently in each hopping period. If any two channel groups hop to the same frequency band, then a collision occurs.

Suppose that there are N_c channel groups with same bandwidth hop over the available hopping spectrum with bandwidth B, and the spectrum can be evenly partitioned by N frequency bands with bandwidth B/N. The assumptions are that each frequency band is used with equal probability, and all channel groups are independent, then each channel group only transmits over one frequency band. Then the collision probability can be written as

$$\begin{aligned} P_c &= 1 - (1 - \frac{\frac{B}{N}}{B})^{N_c-1} \\ &= 1 - (1 - \frac{1}{N})^{N_c-1} \end{aligned} \tag{4}$$

Let $N = 80$ as an example to demonstrate the relationship between the collision probability and the number of hopping channel groups, which is shown in Fig. 4. It can be observed that the collision probability becomes dramatically high as the number of hopping channel groups increases. The low spectral efficiency due to collision effect severely limits the number of channel groups that can be supported by the system.

Since the proposed hopping pattern scheme has the features that a channel group transmits over non-overlapping frequency bands, and no frequency band is left idle; theoretically, the spectral efficiency is 100%. It suggests a significant advantage comparing to the low spectral efficiency of FHMA that conventionally supports multiple hopping groups.

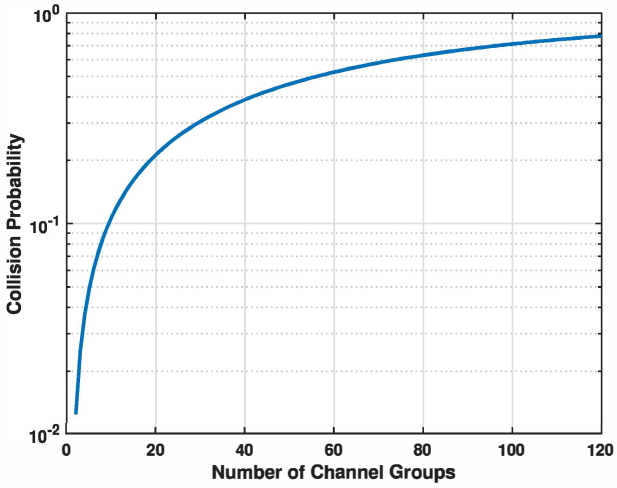

Fig. 4. Collision probability versus number of hopping channel groups

V. Simulation Results

In this section, simulation results are provided to demonstrate the performance of the proposed CGH scheme.

Channel Group Hopping: Fig. 5 demonstrates the channel group hopping over 15 hopping periods. In the simulation, there are 3 channel groups with different bandwidths $B_0 =$ 20MHz (blue), $B_1 =$ 40MHz (brown), and $B_2 =$ 60MHz (pink), respectively. It can be observed that each channel group pseudorandomly hops to a different frequency band in each hopping period, and all channel groups transmit on non-overlapping portions of the hopping spectrum.

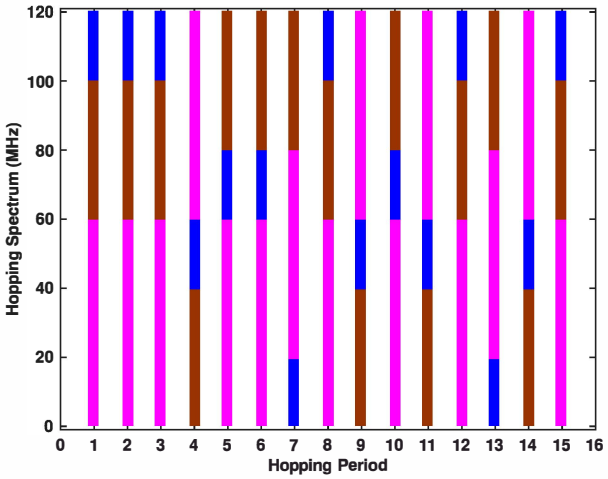

Fig. 5. Channel group hopping demonstration

Symbol Error Rate (SER) Performance: In this simulation, we compare the conventional frequency hopping scheme with the proposed channel group hopping scheme by plotting the SER versus the signal-to-noise ratio (SNR) over AWGN channel. Quadrature phase shift keying (QPSK) symbols are

simulated based on DVB-S2 waveforms [24] that are adopted by PTW. For a simple comparison, channel groups with same bandwidth are assumed for both systems. Fig. 6 suggests that the proposed CGH scheme significantly outperforms the conventional frequency hopping scheme because the collision brings a severe negative effect to the BER performance of the conventional frequency hopping scheme.

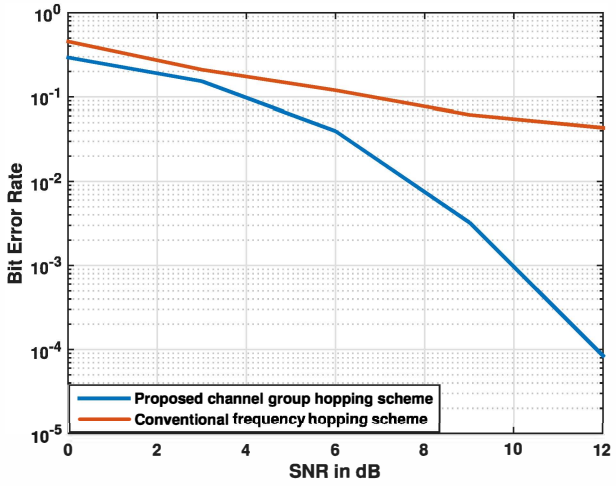

Fig. 6. SER comparison between proposed channel group hopping and conventional frequency hopping

VI. Conclusion

In this paper, we propose a channel group hopping pattern generation algorithm corresponding to the requirements of the PTW system. LFSR first generates the PN sequence, then we encrypt the PN sequence as plaintext by using AES algorithm to produce a ciphertext. After that, the channel group index permutation scheme is applied to the ciphertext to ensure that different channel groups always transmit on non-overlapping frequency bands over the hopping spectrum. The spectral efficiency is investigated to theoretically demonstrate the advantage of the proposed scheme. Simulation results are provided to further illustrate that the proposed CGH scheme outperforms the conventional frequency hopping scheme in supporting multiple channel groups for PTW system.

VII. Acknowledgments

This research was partly supported by the United States Air Force under contract number FA9453-14-C-0017 and FA9453- 15-C-0401. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the United States Air Force.

References

[1] K. Lee, T. Emami, Y. Ibdah, Y. Bi, and L. Li, "Cooperative distributed miso wireless relay networks under jamming environments with power constraints," in *Computational Intelligence, Communication Systems and Networks (CICSyN), International Conference on*, Bali, Indonesia, 2011, pp. 84 – 88.

[2] W. Xiong, A. Mukherjee, and H. M. Kwon, "MIMO cognitive radio user selection with and without primary channel state information," *IEEE Transactions on Vehicular Technology*, pp. 985–991, Feb. 2016.

[3] W. Xiong, A. Mukherjee, and H. M. Kwon, "Underlay MIMO cognitive radio downlink scheduling with multiple primary users and no CSI," in *IEEE conference VTC*, Glasgow, Scotland, 2015.

[4] G. Wang, K. Pham, E. Blasch, T. M. Nguyen, D. Shen, X. Tian, and G. Chen, "Cognitive radio unified spectral efficiency and energy efficiency trade-off analysis," in *Military Communications Conference, MILCOM*, 2015.

[5] S. Wei, D. Shen, L. Ge, W. Yu, E. Blasch, K. Pham, and G. Chen, "Secured network sensor-based defense system," in *SPIE Defense+Security*, 2015, 946909-946909-7.

[6] W. Yu, S. Wei, G. Ma, X. Fu, and N. Zhang, "On effective localization attacks against internet threat monitors," in *IEEE International Conference on Communications (ICC)*, 2013.

[7] L. Li, Y. Ding, J.-K. Zhang, and R. Zhang, "Blind detection with unique identification in two-way relay channel," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2640–2648, Jul. 2012.

[8] Y. Ding, L. Li, and J-K. Zhang, "Blind transmission and detection designs with unique identification and full diversity for noncoherent two-way relay networks," *IEEE Tran. Vehicular Technology*, vol. 63, pp. 3137–3146, 2014.

[9] L. Li, G. Wang, G. Chen, H.-M. Chen, and K. Pham E. Blasch, "Robust airborne image transmission using joint source-channel codintraffic UEP," in *IEEE Aerospace Conference*, 2016.

[10] S. Xia and P. Wang, "Distributed throughput optimal scheduling in the presence of heavy-tailed traffic," in *IEEE International Conference on Communications (ICC)*, 2015, pp. 3490–3496.

[11] A. Mukherjee, W. Xiong, and H. Kwon, "CSI-unaware scheduling for coexistence of mimo-ofdma device-to-device links and cellular mobile terminals," in *IEEE Millitary Communication Conference (MILCOM)*, 2015.

[12] A. Ephremides, J. E. Wieselthier, and D. J. Baker, "A design concept for reliable mobile radio networks with frequency hopping signaling," *Proc. IEEE*, vol. 75, pp. 56–73, 1987.

[13] E. Geraniotis and M. Pursley, "Error probabilities for slow-frequency-hopped spread-spectrum multiple-access communications over fading channels," *IEEE Transactions on Communications*, vol. 30, pp. 996–1009, 1982.

[14] E. Chiprout and M. S. Nakhla, "Analysis of interconnect networks using complex frequency hopping (CFH)," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 14, pp. 186–200, 1995.

[15] P. Udaya and M. U. Siddiqi, "Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings," *IEEE Transactions on Information Theory*, vol. 44, pp. 1492 – 1503, 1998.

[16] K. W. Halford and M. Brandt-Pearce, "Multistage multiuser detection for fhma," *IEEE Transactions on Communications*, vol. 48, pp. 1550–1562, 2000.

[17] M. C. Valenti and X. Xiang, "Constellation shaping for bit-interleaved LDPC coded APSK," *IEEE Transactions on Communications*, vol. 60, no. 10, pp. 2960–2970, Oct. 2012.

[18] X. Xiang and M. C. Valenti, "Closing the gap to the capacity of APSK: Constellation shaping and degree distributions," in *Networking and Communications (ICNC)*, San Diego, CA, 2013, pp. 691–695.

[19] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hoppingpart i: System design," *IEEE Transactions on Wireless Communications*, vol. 12, pp. 70–79, 2013.

[20] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping-part ii: Capacity analysis under disguised jamming," *IEEE Transactions on Wireless Communications*, vol. 12, pp. 80–88, 2013.

[21] L. Zhang, J. Ren, and T. Li, "Spectrally efficient anti-jamming system design using message-driven frequency hopping," in *2009 IEEE International Conference on Communications*, 2009.

[22] D. Muthiah and A. A. B. Raj, "Implementation of high-speed LFSR design with parallel architectures," in *International Conference on Computing, Communication and Applications*, 2012.

[23] N. Sklavos and O. Koufopavlou, "Architectures and VLSI implementations of the AES-proposal Rijndael," *IEEE Transactions on Computers*, vol. 51, pp. 1454 – 1459, 2002.

[24] X. Xiang and M. C. Valenti, "Improving DVB-S2 performance through constellation shaping and iterative demapping," in *Military Communication Conference (MILCOM)*, Baltimore, MD, 2011, pp. 549–554.