Blind Estimation for the Generation Polynomial of FHSS Signals using Time Frequency Analysis

Ganghyuk Jeon, Yooncheol Choi, and Dongweon Yoon*
Department of Electronic Engineering
Hanyang University
Seoul, Korea
*dwyoon@hanyang.ac.kr

***Abstract*—The escalation of worldwide conflicts and accessibility of unmanned aerial vehicles (UAVs) have led to the increase of various security concerns. To implement effective protective measures against unauthorized drones, it is crucial to blindly estimate the generation polynomial of the frequency hopping spread spectrum (FHSS) signals, which are commonly used in UAVs. This paper presents a robust algorithm for the blind estimation of generation polynomials with partial observation of the signal hopping period, utilizing time frequency images (TFI) and unique preprocessing methods to accurately and efficiently extract the hopping pattern. The TFI is segmented into each hopping region, which undertakes noise reduction via temporal marginalization independently. Subsequently, the noise-reduced image is standardized, clipped along the frequency axis for pattern enhancement. Then, the analysis of the preprocessed image allows for the identification of the hopping pattern, which can be used to reconstruct the generation polynomial by simple linear operations. Simulation results show that the proposed algorithm reduces the required signal duration for identifying the generation polynomial and enhances estimation accuracy.**

***Index Terms*—frequency hopping spread spectrum, time-frequency image, blind estimation**

I. Introduction

In non-cooperative contexts, such as spectrum surveillance and cognitive radio systems, the receiver should operate without any prior information about the transmitter. To recover the received signal and retrieve the original information, the receiver must autonomously estimate key communication parameters. These include determining the modulation scheme [1], [2], identifying the interleaver pattern [3], [4], recognizing the scrambler configuration [5], [6], detecting the spreading sequence [7], [8], and so on. Particularly in frequency hopping spread spectrum (FHSS) systems, estimating the generation polynomial and the resulting hopping pattern is crucial, as these elements define the frequency transitions and directly impact the effectiveness of signal interception and analysis.

This need for blind estimation becomes even more pressing in the context of growing security concerns surrounding the use of unmanned aerial vehicles (UAVs). With the escalation of numerous global conflicts in the recent decade, the use of UAVs have increased concerns over privacy violations, explosive attacks against civilians, smuggling, and unauthorized surveillance of restricted sites [9]. As UAV technology becomes more accessible in the commercial market, the threat posed by these devices in malicious hands has been increasingly noted. To address this issue, because UAVs often employ FHSS systems, various jamming techniques targeting FHSS have been proposed as countermeasures against unauthorized drones. A wideband jammer disrupts signals by emitting high-energy interference across entire frequency bands, effectively overwhelming the target signal, but it faces the limitation of excessive energy usage. On the other hand, a random jammer degrades the signal by rapidly hopping across multiple frequencies, but its effectiveness can be reduced if the hopping pattern is unpredictable or too fast. Additionally, a reactive jammer detects the frequencies being used by the target signal and interferes on those frequencies to disrupt communication, yet it requires high reaction speeds and can be costly to implement [10] . Limitations of the jamming process can be effectively overcome by estimating the generation polynomial of the FHSS signal, as exposing the hopping pattern can drastically reduce the cost of jamming to effectively disrupt communication between the UAV and the controller [11] . Sequential estimators, which estimate parameters of a system by processing data points incrementally as they are observed, can, in theory, contribute to the estimation of the hopping pattern of the FHSS system, but they face significant challenges, especially in noisy environments. However, by utilizing TFI and advanced image processing techniques, it is possible to adopt a similar estimation mechanism that is more robust in such conditions.

Conventional studies generally utilize time-frequency image (TFI) to estimate the hopping pattern, focusing on capturing the whole hopping period of the FHSS signal [12]–[14]. Various statistical methods were adopted to extract each hopping frequency to reconstruct the hopping pattern. Reference [12] utilized smooth windowed Wigner-Ville distribution (SWWVD) and the instantaneous frequency moment method to estimate the hopping frequencies and the hopping interval. Reference [13] on the other hand, based its estimation on the combination of short-time Fourier transform (STFT) and smoothed pseudo-Wigner-Ville distribution (SPWVD) to estimate the duration, center instant and frequency parameters of each hop for synchronous and asynchronous environments.

This work was supported by Korea Research Institute for defense Technology planning and advancement (KRIT) grant funded by the Korea government (DAPA (Defense Acquisition Program Administration)) (No. KRIT-CT-22021, Space Signal Intelligence Research Laboratory, 2022)

Additionally, reference [14] utilized simple STFT to estimate the next hopping frequency with a limited observation window and deep learning models.

While previous works have proved the effectiveness and versatility of TFIs in the blind estimation of FHSS system, there is still room for further improvement in both the image preprocessing and analysis methods. This paper presents a robust algorithm for the blind estimation of generation polynomials with partial observation of the signal hopping period, utilizing TFIs and unique preprocessing methods to accurately and efficiently extract the hopping pattern. The TFI is segmented into each hopping region, which undertakes noise reduction via temporal marginalization independently. Subsequently, the noise-reduced image is standardized and clipped along the frequency axis for pattern enhancement. Then, the analysis of the preprocessed image allows for the identification of the hopping pattern, which can be used to reconstruct the generation polynomial by simple linear operations. The proposed algorithm notably reduces the required signal duration for identifying the generation polynomial, making it more efficient and suitable for real-time applications. Furthermore, simulation shows that it enhances estimation accuracy, ensuring robust and reliable detection of unauthorized UAVs.

The structure of this paper is as follows; Section II explains the FHSS system model. Section III describes the TFI preprocessing method and the generation polynomial estimation algorithm. Section IV presents the the simulation results. Finally, Section V provides the conclusion of this paper.

II. System Model

The FHSS system model for the target UAV is comprised of a pseudo-noise (PN) sequence generator, a frequency synthesizer and a FSK modulator. Figure 1. shows the FHSS communication system diagram.

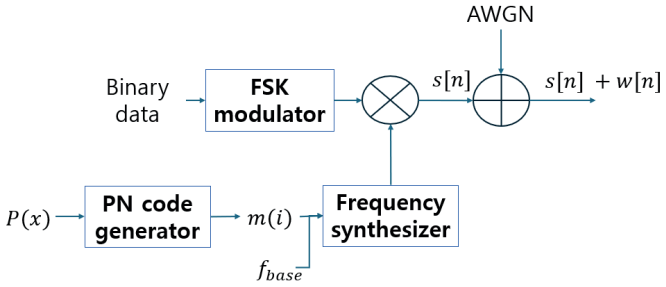


Fig. 1: Block diagram of FHSS system

The FH pattern determines the frequency levels of the FHSS signal. It is generated by a generation polynomial, denoted as $P(x) = 1 + c_1 x + \cdots + c_n x^n$. The coefficient matrix $\mathbf{C} = [c_1, c_2, \ldots, c_n]^T$ determines the linear feedback shift register (LFSR) and the binary state of the registers for each shift determines the hopping pattern, denoted as $m(i)$. The sequence is then mapped to a frequency hopping pattern by multiplying $m(i)$ by a fixed frequency f_{base}. The resulting frequency level for the i-th step in the hopping pattern is expressed as follows:

$$f_h(i) = f_{\text{base}} \times m(i). \tag{1}$$

This mapping directly ties the hopping pattern to the underlying m-sequence, providing a pseudo-random yet deterministic sequence of frequencies for the FHSS system. The binary data is modulated by FSK, and subsequently, this modulated signal is combined with a series of frequency hopping levels to generate a FHSS signal. If the data bit is '1', the signal is modulated with a positive frequency shift; if the bit is '0', the signal is modulated with a negative frequency shift. This results in a fully modulated FHSS signal, where each bit is transmitted on a different frequency channel as determined by the PN sequence.

The modulated signal $s_i[n]$ for the i-th bit is expressed as follows:

$$s_i[n] = \cos\left\{2\pi f_{h,\{(i \mod L)+1\}} n T_e - (2d_i - 1)2\pi f_1 n T_e\right\}. \tag{2}$$

The data sequence is denoted as $d_i \in \{0, 1\}$. The time duration of one bit is represented by the time index n and the sampling period T_e, and the frequency of each hop is given by $\{f_{h,k}\}$. L is the length of the frequency hopping sequence, and $f_{h,\{(i \mod L)+1\}}$ is the frequency selected from the hopping pattern for the i-th bit. f_1 is the frequency shift for BFSK modulation. The intercepted FHSS signal $y[n]$ can be written as:

$$y[n] = s[n] + w[n], \tag{3}$$

where $w[n]$ is the additive white Gaussian noise introduced by the channel.

III. Estimation Algorithm

This section explains the proposed algorithm for the estimation of FHSS generation polynomial by utilizing TFI. Figure 2 illustrates the block diagram of the proposed algorithm.

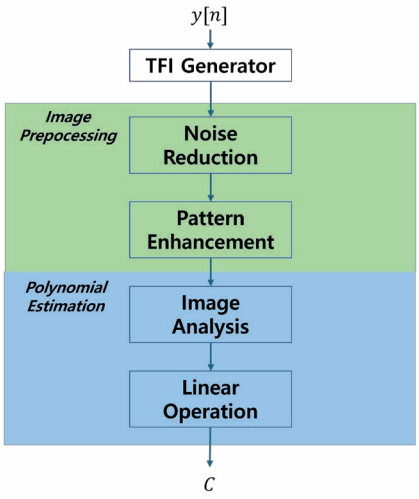


Fig. 2: Block diagram of the estimation process

First, the received signal is processed to generate a TFI which represents the frequency hops over time and is essential for analyzing the hopping pattern. Subsequently, the TFI undergoes advanced image preprocessing techniques, such as noise reduction and pattern enhancement, to improve the quality of the image. By analyzing the TFI, the sequence of frequency levels and their timing are identified, enabling the reconstruction of the generation polynomial.

A. Image Preprocessing

To begin the estimation process, a TFI is generated by STFT. STFT is utilized due to its relatively low computational costs [15]. STFT of the received signal $y[n]$ is defined as follows:

$$D_{l,m} = \sum_{k=mR}^{mR+M-1} y[k]\, w[k-mR]\, \exp\left(-j\frac{2\pi}{M}lk\right), \quad (4)$$

where $D_{l,m}$ represents the STFT of $y[k]$ at the frequency index l and time index m; the function $w[k]$ denotes the window applied to the signal; and R indicates the number of samples that overlap between consecutive time segments. To visualize the STFT of the received radar signal, we convert $D_{l,m}$ into a spectrogram by computing the square of the amplitude of the STFT, expressed as $Y_{l,m} = |D_{l,m}|^2$.

The spectrogram is then normalized using min-max scaling to ensure the values lie within the gray-scale range of [0,1] and is resized by nearest-neighbor interpolation to unify signal scale and TFI size for further processing. The normalization is defined as follows:

$$G_{l,m} = \frac{Y_{l,m} - \min\limits_{l,m}(Y_{l,m})}{\max\limits_{l,m}(Y_{l,m}) - \min\limits_{l,m}(Y_{l,m})}, \quad (5)$$

where $G_{l,m}$ is the converted gray-scale image. The resized grayscale spectrogram is represented as $I(u,v)$. Here, u and v represent the row and column index of the image, respectively.

Subsequently, to ensure accurate estimation, noise reduction and pattern enhancement are considered for image preprocessing techniques. For noise reduction, the process is performed independently for each hop to focus on each frequency level and its environment. As such, the image is segmented by each hop duration and marginalized along the time axis. Let $I^i_{\text{seg}}(u,v)$ represent the i-th segment of the image, defined as:

$$I^i_{\text{seg}}(u,v) = \begin{cases} I(u,v), & \text{if } v_i \le v < v_{i+1} \\ 0, & \text{otherwise,} \end{cases} \quad (6)$$

where v_i is the boundary that defines the segment by hop duration.

A marginalized vector from the segment provides information about the frequency levels occupied by the FHSS signal. The marginalized vector g_i for the i-th segment is derived as follows:

$$g_i = \sum_v I^i_{\text{seg}}(u,v). \quad (7)$$

Since the signal is concentrated in a limited range of frequency levels, the marginalized vector g_i will have higher values in the signal frequency levels compared to the noise-only frequencies. For noise reduction, each segment $I^i_{\text{seg}}(u,v)$ is processed by multiplying each column with its corresponding value in the marginalized vector, denoted as follows:

$$R^i_{\text{seg}} = \text{diag}(g_i) \times I^i_{\text{seg}}. \quad (8)$$

Here, $\text{diag}(g_i)$ represents a diagonal matrix where the major diagonal is filled with g_i. The concatenation of each noise-reduced segment $R(u,v)$ exhibits pronounced reduction in pixel values in the noise-only range compared to the signal component range.

Finally, the noise-reduced image undergoes standardization in the frequency axis and clipping under average pixel value to enhance the hopping patterns. The standardization and clipping process is given as follows:

$$S(u,v) = \frac{R(u,v) - \mu_v}{\sqrt{\sigma_v^2}}, \quad (9)$$

$$E(u,v) = \begin{cases} S(u,v), & \text{if } S(u,v) \ge 0 \\ 0, & \text{if } S(u,v) < 0. \end{cases} \quad (10)$$

Here, $S(u,v)$ and $E(u,v)$ denote the standardized and clipped image, respectively. μ_v denotes the mean and σ_v the variance of the v-th column of R. This process accentuates the patterns in $R(u,v)$.

Figure 3 demonstrates that the processed image exhibits less noise and an accentuated frequency hopping pattern compared to the raw spectrogram.

(a) Raw spectrogram (b) Preprocessed image

Fig. 3: Comparison between preprocessed image and raw spectrogram

B. Polynomial Estimation

The next step requires extracting the hopping frequency levels through the analysis of each segment $E^i_{\text{seg}}(u,v)$, to estimate the generation polynomial. This process begins by summing the columns of each hop duration segment, allowing us to identify the frequency index with the highest value, as shown in (11) and (12).

$$M^i(f) = \sum_v E^i_{\text{seg}}(u,v) \quad (11)$$

$$f^i_{\max} = \arg\max M^i(f) \quad (12)$$

Here, $M^i(f)$ represents the summed values of each frequency column for the i-th segment. The frequency index corresponding to the maximum of $M^i(f)$ is denoted as f^i_{max}. From the above process, the set $\{f_{\text{max}}\}$ containing frequency levels for all segments is generated. To determine the spacing between frequency levels, a recursive process is used to form difference sets between adjacent elements until a set includes a zero. Define $\{\Delta f_1\}$ to be a set of all absolute differences between adjacent elements of $\{f_{\text{max}}\}$:

$$\Delta f_1 = \left\{ \left| f^{(i+1)}_{\text{max}} - f^i_{\text{max}} \right| : 1 \leq i < m \right\}. \tag{13}$$

Recursively, for each $n \geq 2$, define the set $\{\Delta f_n\}$ as the set of all differences between adjacent elements of the set $\{\Delta f_{n-1}\}$. Continue this process until a set is reached where $\{\Delta f_k\}$ contains the element zero.

Once the sequence $\{\Delta f_n\}$ reaches the termination point, d_{min} is defined as the minimum non-zero element among all the sets $\{\Delta f_1\}, \{\Delta f_2\}, \ldots, \{\Delta f_k\}$.

$$d_{\text{min}} = \min \left(\bigcup_{i=1}^{k} \Delta f_i \setminus \{0\} \right) \tag{14}$$

The value d_{min} is the estimation of f_{base} converted to column index. As such, f^i_{max} is is divided by d_{min} to estimate the value of the m-sequence, as shown in (15).

$$m_{\text{est}}(i) = \left\lfloor \frac{f^i_{\text{max}}}{d_{\text{min}}} \right\rfloor \tag{15}$$

The set of estimated $m_{\text{est}}(i)$ represents the integer interpretation of the binary state of the registers for each shift of the LFSR. Given a known polynomial degree n, a linear equation for estimating the coefficients of the generating polynomial [16] can be constructed using $n+1$ consecutive $m_{\text{est}}(i)$ as follows:

$$\begin{aligned} &\mathbf{IC} = \mathbf{O}, \\ &\mathbf{I} = \begin{bmatrix} i_{11} & i_{12} & \cdots & i_{1n} \\ i_{21} & i_{22} & \cdots & i_{2n} \\ \vdots & & \ddots & \vdots \\ i_{n1} & i_{n2} & \cdots & i_{nn} \end{bmatrix}, \\ &\mathbf{C} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}, \ \mathbf{O} = \begin{bmatrix} i_{21} \\ i_{31} \\ \vdots \\ i_{(n+1)1} \end{bmatrix}. \end{aligned} \tag{16}$$

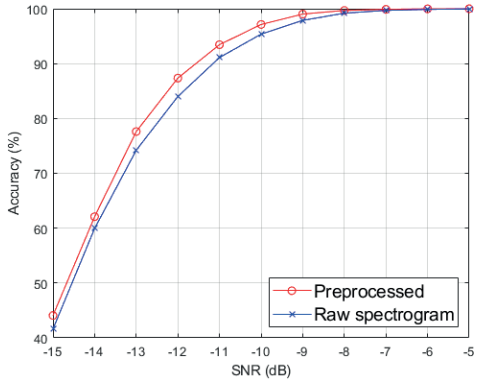
Here, each row of $\mathbf{I}$ represents the binary form of $m_{\text{est}}(i)$ and $\mathbf{C}$ represents the generation polynomial coefficient. By the nature of the LFSR, the output $\mathbf{O}_k = \mathbf{I}_{(k+1)1}$. Finally, the coefficients are estimated using matrix inversion if the matrix $\mathbf{I}$ is non-singular: $\mathbf{C} = \mathbf{I}^{-1}\mathbf{O}$.

IV. Estimation Performance

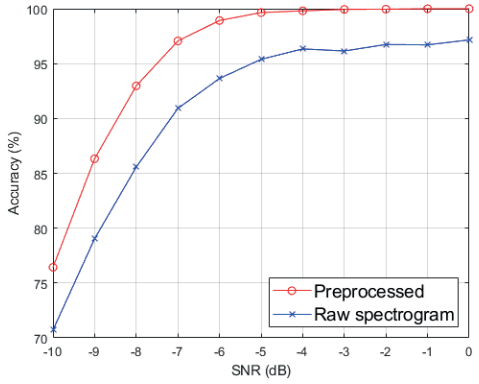
In this section, we describe the various parameters for the simulation data and present the estimation performance of the proposed FHSS generation polynomial estimation under various SNR conditions. The parameters used for the FHSS signal generation are detailed in Table 1. The parameters include a data rate of 1000 bits/s and a hopping rate of 1 hop/bit. The signals were sampled at a frequency of 1 MHz, with a minimum hop frequency set at 10 KHz. The TFI method used was the 'pspectrum' function, which is a type of spectrogram generation method, and the generated images were resized to a resolution of 400 x 400 pixels. For each SNR value, the estimation process was repeated 10,000 times to ensure statistical reliability.

TABLE I: Simulation parameters

Parameter	Value
Data rate	1000 bits/s
Hopping rate	1 hop/bit
Sampling frequency	1 MHz
Minimum hop frequency	10 kHz
TFI method	pspectrum
Image size	400 x 400 pixels
Estimation count	10000 count/SNR



(a) $n = 3$



(b) $n = 4$

Fig. 4: Estimation accuracy of generation polynomial

We depict the comparative results of generation polynomial estimation accuracy using the proposed algorithm on both raw and preprocessed spectrogram images under varying signal conditions in Figure 4. In the first set of simulations, illustrated in Figure 4(a), the polynomial degree was set to $n = 3$, and

the signal-to-noise ratio (SNR) was varied between -15 dB and -5 dB. This range was selected to replicate challenging conditions with high noise levels. Despite these conditions, preprocessing the spectrogram image led to a 3% improvement in image quality compared to the raw spectrogram, demonstrating the effectiveness of the preprocessing steps in enhancing image clarity, which is crucial for accurate polynomial estimation. Notably, the estimation was successful with only 57% of the hopping period observed, highlighting the algorithm's efficiency and robustness even with partial data.

In the second set of simulations, as illustrated in figure 4(a), the polynomial degree was increased to $n = 4$, and the SNR values were adjusted to range from -10 dB to 0 dB. This adjustment reflects a scenario where the signal is stronger relative to the noise, yet still presents a considerable challenge for accurate estimation. The results exhibit a significant enhancement in estimation accuracy, with the preprocessed image showing an improvement of over 12% compared to the raw spectrogram. This considerable improvement highlights the effectiveness of the preprocessing techniques applied, which include noise removal, segmentation, and pattern enhancement. The preprocessing not only improves the visual quality of the image but also enhances the algorithm's ability to detect and accurately estimate the underlying polynomial. In this scenario, the estimation was accomplished by analyzing only 33% of the entire hopping pattern, which is a substantial reduction compared to the first simulation set. This reduction in required observation time demonstrates the algorithm's increasing efficiency with higher polynomial degrees.

These simulation results collectively validate the proposed algorithm's capability to accurately estimate the generating polynomial even when only a portion of the hopping period is observed. The reduced requirement for signal duration is particularly significant, as it suggests that the algorithm can operate effectively in real-time applications where data acquisition may be limited by time or other constraints. Furthermore, the use of TFI combined with unique preprocessing techniques, such as noise removal through segmentation and pattern enhancement, plays a crucial role in the algorithm's success. These techniques not only improve the quality of the images used for analysis but also significantly boost the estimation accuracy compared to methods that rely on raw spectrogram images. The robustness and flexibility of the approach, demonstrated under various simulated conditions, indicate that this algorithm is a dependable tool for estimating the FHSS generating polynomial.

V. Conclusion

In this paper a robust algorithm for the blind estimation of generation polynomials of FHSS with partial observation of the signal hopping period and TFI utilization was proposed. The TFI was segmented into each hopping region, which undertakes noise reduction via temporal marginalization independently. Subsequently, the noise-reduced image was standardized, clipped along the frequency axis for pattern enhancement. Then, the analysis of the preprocessed image allowed for the identification of the hopping pattern, which can be used to reconstruct the generation polynomial by simple linear operations. It was demonstrated through simulations that the proposed algorithm accurately estimates the generation polynomial, even when only a portion of the hopping period is observed, reducing estimation time significantly. Furthermore, by utilizing unique preprocessing methods, it enhanced the estimation accuracy compared to raw spectrogram image. The approach performed well under various conditions, making it a reliable tool for the estimation of the generation polynomial of FHSS signals. Further research is needed to accurately estimate the polynomial degree and signal bandwidth without prior knowledge, making the algorithm more versatile.

References

[1] J. Lee, J. Kim, B. Kim, D. Yoon, and J. Choi, "Robust automatic modulation classification technique for fading channels via deep neural network," *Entropy*, vol. 19, no. 9, p. 454, Aug. 2017.

[2] G. Song, M. Jang, and D. Yoon, "Automatic modulation classification for OFDM signals based on CNN with α-softmax loss function," *IEEE Trans. Aerosp. Electron. Syst.*, pp. 1-8, May 2024 (Early Access).

[3] Y. Jung, M. Jang, and D. Yoon, "Improved method for blind interleaver parameter estimation using matrix multiplication from scant data," *IEEE Access*, vol. 9, pp. 138209-138214, Oct. 2021.

[4] M. Jang, G. Kim, Y. Kim, and D. Yoon, "Blind estimation of interleaver parameter with a limited number of data," *IEEE Access*, vol. 8, pp. 69160-69166, Apr. 2020.

[5] M. Jang, G. Kim, D. Kim, and D. Yoon, "Blind interleaver parameter estimation from scant data," *IEEE Access*, vol. 8, pp. 217282-217289, Dec. 2020.

[6] Y. Kim, J. Kim, J. Song, and D. Yoon, "Blind estimation of self-synchronous scrambler using orthogonal complement space in DSSS systems," *IEEE Access*, vol. 10, pp. 66522-66528, Jun. 2022.

[7] C. Bouder, S. Azou, and G. Burel, "Performance analysis of a spreading sequence estimator for spread spectrum transmissions," *J. Franklin Inst.*, vol. 341, no. 7, pp. 595-614, Nov. 2004.

[8] Y. Choi, D. Kim, M. Jang, and D. Yoon, "Spreading sequence blind estimation in DSSS system using gradient ascent method," in *Proc. Int. Telecommun. Netw. Appl. Conf.*, Melbourne, Australia, Dec. 2023, pp. 76-79.

[9] G. Abro, S. Zulkifli, R. Masood, V. Asirvadam, and A. Laouiti, "Comprehensive review of UAV detection, security, and communication advancements to prevent threats," *Drones*, vol. 6, no. 10, p. 284, Oct. 2022.

[10] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2001.

[11] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 16–30, Jan. 2012.

[12] A. Kanaa and A. Z. Shaameri, "A robust parameter estimation of FHSS signals using time frequency analysis in a non-cooperative environment," *Phys. Commun.*, vol. 26, pp. 9-20, Feb. 2018.

[13] D. Zhang, Y. Shang, X. Liang, and J. Lin., "Efficient blind estimation of parameters for multiple frequency hopping signals via single channel," in *Proc. IEEE Int. Conf. Autom. Electron. Electr. Eng*, Shenyang, China, 2022, pp. 1063-1069.

[14] P. Thiele, L. Bernadó, D. Löschenbrand, B. Rainer, C. Sulzbachner, M. Leitner, and T. Zemen, "Machine learning based prediction of frequency hopping spread spectrum signals," in *Proc. Annu. Int. Symp. Pers. Indoor Mobile Radio Commun.*, Toronto, ON, Canada, 2023, pp. 1-6.

[15] E. G. Strangas, S. Aviyente, and S. S. H. Zaidi, "Time-frequency analysis for efficient fault diagnosis and failure prognosis for interior permanent-magnet AC motors," *IEEE Trans. Ind. Electron.*, vol. 55, no. 12, pp. 4191–4199, Dec. 2008.

[16] W. Jin, J. Wang, H. Liao, and L. Gan, "Estimation of primitive polynomial for m-sequence with finite sequence length," in *Proc. IEEE Adv. Inf. Technol. Electron. Autom. Control Conf.*, Chongqing, China, 2018, pp. 1-4.