Analysis the Reliability Capability of Cognitive Frequency Hopping Communication System

Chenxi Li*, Peihan Qi*†, Danyang Wang*, and Xiaoyu Zhou*
*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China
†Collaborative Innovation Center of Information Sensing and Understanding
Email: chenxili@stu.xidian.edu.cn; phqi@xidian.edu.cn; dywang@xidian.edu.cn; zxy0686@126.com

***Abstract*—In this paper, we propose a method that can effectively measure the reliability capability of cognitive frequency hopping (CFH) communication systems. Considering that various malicious interference devices and advanced interference technologies have appeared in the wireless communication environment, a novel method called CFH has been proposed recently to effectively resist the interference devices. This method can evaluate the occupation of frequency hopping frequency slots, and thus dynamically adjust the system parameters based on the evaluation results. However, we note that the existing literature only shows that the system is reliable, but few work has been done to analyze the reliability of the CFH system and the factors affecting the reliability. Therefore, by analyzing the effects of false alarm probability, missed detection probability, and communication link convergence delay, we obtain analytical expressions to evaluate reliability. Simulation results evaluate the proposed method.**

***Index Terms*—Cognitive frequency hopping (CFH), reliability capability, false alarm probability, missed detection probability, and communication link convergence delay.**

I. Introduction

Wireless communication, as a method of long-distance information transmission that can be carried without conductors or cables, has been widely used in many fields (such as cellular networks, industrial production, etc.). However, while the wireless communication technology is showing a booming trend, the risk that the information it brings is easily interfered or intercepted has also caused widespread concern [1]–[4]. Wireless communication is different from traditional wired communication, and it mainly relies on electromagnetic waves to transmit signals. Due to the open nature of wireless channels and the broadcast nature of radio transmission, information is extremely vulnerable to external interference during transmission. In addition to sources of malicious interference in wireless communication environments, signals from unauthorized users are also considered important sources of interference. Moreover, when multiple wireless devices are working simultaneously, signals sent by other authorized users may also cause interference to the communication link, thereby reducing the security and reliability of wireless communication. With the increase of the amount of private information carried by communication networks, the interception technology has also been continuously improved [5]–[7], and the importance of information security has increased to an unprecedented level.

Focusing on the these security threats and challenges, research on the anti-interference performance of wireless communications has received extensive attention in the past few years. In communication systems based on different application fields, there are many anti-interference schemes [8]–[13], which can be divided into three categories. The first type comes from the spatial domain, such as *beamforming technology* for directional transmission [8], [9]. However, as the amount of high-rate multimedia wireless services carried by limited spectrum resources is rapidly increasing, the electromagnetic environment is changing in a more complex and changeable direction. These factors pose great challenges to the implementation of this method. The second type comes from the time domain, such as *time-hopping spread spectrum communication* [10], [11]. These methods achieve the purpose of anti-interference by expanding the signal frequency band, but at the cost of available resources in the time domain. The third type comes from the frequency domain, such as *frequency hopping* (FH) *technology* [12], [13]. Whereas its performance is limited by the fixed parameters (e.g., the frequency slot number, the frequency gap and bandwidth, etc.), it is difficult to resist the advanced dynamic interference signals.

Obviously, faced with the situation that the shortage of spectrum resources is becoming more and more serious, the aforementioned schemes cannot adapt to the highly complex and dynamic electromagnetic environment. In addition, a variety of new interference technologies have emerged, and the ability to interfere with devices has continued to increase. Therefore, in order to effectively resist the influence of interfering devices on the wireless communication system, a new method called *cognitive frequency hopping* (CHF) [14]–[16] has been recently proposed. This method can quickly determine the FH frequency slots affected by interference, and dynamically adjust parameters based on the evaluation results, thereby effectively improving the anti-interference performance of FH communications. However, because the existing literature only shows that the CFH system has anti-interference ability, the anti-interference ability of the system and the factors affecting the anti-interference performance are rarely analyzed. Therefore, we also propose a method for measuring the anti-interference ability of CFH communication systems.

In this paper, we propose a transmission scheme of the CFH communication system. Meanwhile, we derive the analytic expression of reliability tolerance by analyzing the effect

EAI MOBIMEDIA 2020, August 27-28, Harbin, People's Republic of China

DOI 10.4108/eai.27-8-2020.2294328

of false alarm probability, missed detection probability, and communication link convergence delay. Compared with the literature that lacks CFH communication system performance analysis, our analysis provides a theoretical basis for studying complex and practical anti-interference communication systems. In addition, according to our theoretical derivation, the reliability capability of CFH systems can be optimized by adjusting relevant parameters to meet different requests.

The remainder of this paper is organized as follows. The infrastructure model is shown in Section II. Then Section III analyzes the anti-interference performance of CFH communication system. After that, the simulation results are provided in Section IV. Finally, Section V draws the conclusion of this paper.

II. Infrastructure Modeling

Based on the available FH communication system models and cognitive radio communication system models [14]–[17], we construct a typical CFH communication system model in Fig. 1.

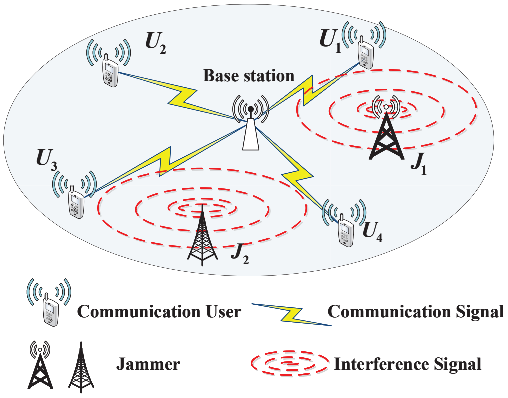

Fig. 1. System model.

In our constructed communication scenario, multiple communication users $U_p(p = 1, 2, \cdots, N)$ and different types of interference devices $J_q(q = 1, 2, \cdots, M)$ coexist, which is consistent with the actual communication environment. Without desired and legitimate transmission between authorized users, the useless interference signal may be transmitted randomly by jammer devices, which will seriously affect the communication quality, and even cause information loss, communication link interruption and other negative influences. In order to effectively ensure the security of information transmission and enhance the anti-interference ability of the CFH communication system, a transmission scheme is shown in Fig. 2.

As shown in Fig. 2, the proposed CFH communication system has the communication bandwidth of W, which can be equally divided into n frequency slots. Consequently, a set of frequency slots can be obtained $F = \{f_a \,|a = 1, 2, \cdots, n\}$, and the bandwidth of each frequency slot is $B = W/n$. The interference power, frequency hopping signal power, and noise power within each frequency slot are J_a, S_a, and N_a, respectively. In the CFH system, before the communication user transmits the signal, the occupation of each frequency slot in the wireless channel can be analyzed through the spectrum sensing technology based on the high-order cumulant [18]. Therefore, the channel model can be expressed as

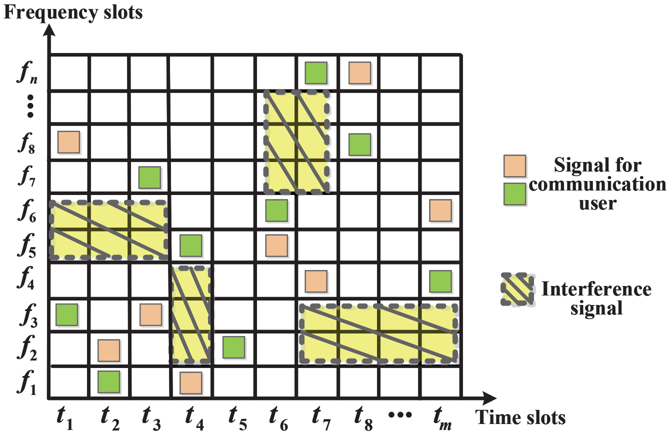

Fig. 2. Transmission strategy.

$$\begin{cases} H_0: \; y(t) = n(t), \\ H_1: \; y(t) = x(t) + n(t), \end{cases} \tag{1}$$

where state H_0 and state H_1 represent the frequency slot is only occupied by the background noise and the presence of the signals transmitted by other users or devices, respectively. At time t, the signals obtained by the sensing system, the transmitted signals of other users on the target frequency slot, and the background noise are indicated by $y(t)$, $x(t)$, and $n(t)$. In addition, $n(t)$ is a complex Gaussian random variable which is characterized by the mean of zero and the variance of α_n^2. It should be pointed out that no matter which sensing method is used, it is impossible to achieve completely accurate spectrum detection. Without loss of generality, there are false alarm (the state without interference is judged to be interference) probability and missed detection (the state with interference is judged as no interference) probability in CFH system's perception of the interference signal in each frequency slot, which are represented by P_f and P_{md} respectively.

According to the high-order cumulant spectrum sensing method [18], the corresponding decision metric value T is compared with the set decision threshold γ, and the detection probability P_{d} and the false alarm probability P_f can be expressed as

$$\begin{cases} P_{\mathrm{d}} = \Pr(T > \gamma \,|H_1\,), \\ P_f = \Pr(T > \gamma \,|H_0\,). \end{cases} \tag{2}$$

Based on the results of spectrum sensing, it can be determined that k $(0 \le k \le n)$ frequency slots in the spectrum set F are occupied by interference signals. The CFH system removes the k interfered frequency slots from the set F, and the set of available frequency slots F_A, which are not occupied by the interference signal, can be determined. To avoid the interference frequency slots and obtain a certain reliability tolerance, the transmitter makes the carrier of the modulated signal occupy the available frequency F_A by up-conversion. The transmitter U_1 can select the frequency slots from F_A to transmit the information by using FH method in each time slot $T = \{t_b\,|b = 1, 2, \cdots, m\}$.

III. Anti-interference performance analysis

According to the CFH communication system constructed in Section II, its working cycle can be divided into four stages: spectrum sensing stage, time synchronization stage, cognitive decision-making stage, and communication stage. Once the FH communication user enters the system, this user begins to continuously perceive the spectrum environment to obtain the available frequency slots set F_A. Subsequently, all the FH communication users in this system adjust the local time of day (TOD) to complete the time synchronization. Combined with the existing method of generating a FH transmission strategy [12]–[15], we can clearly find that these strategy are controlled by the group of FH sequence families. Therefore, based on the idea of block cryptography, a group of basic FH sequences can be generated by controlling the network identification *key* of both communicating parties

$$S^0 = \{\mathrm{s}^0_{a,b}, a = 1, 2, \cdots, n \text{ and } b = 1, 2, \cdots, m\}. \quad (3)$$

It is emphasized that the network identification *key* of the constructed system will be periodically updated from other systems in the wireless communication network, and CFH users can only join the cognitive system with the *key* of this system. Then, using the Round Function to S^0 for y $(y \leq n)$ consecutive iterations as

$$\begin{cases} \mathrm{s}^y_{a,b} & = s^{y-1}_{a,b-1} \oplus key, \\ \mathrm{s}^y_{a,b-1} & = \mathrm{Sbox}j(\mathrm{s}^y_{a,b}) \oplus \mathrm{s}^{y-1}_{a,b}. \end{cases} \quad (4)$$

Therefore, at time b, we can obtain the sequence families $\{S^0, S^1, \cdots, S^y\}$. Consequently, by using the remapping method, the sequence family that generates the control user transmission information can be presented in the form of an algorithm

$$\{X_{a,b}\} = g\ (\mathrm{TOD}_b, key, f_a, \cdots). \quad (5)$$

When the communication user in the CFH system receives the feedback of the spectrum sensing result, they can identify the frequency slots corresponding to the FH sequence and transmit information independently from the available frequency slots F_A.

In addition, since the CFH communication system is obtained by adding cognitive module on the basis of conventional FH communication system, the reliability tolerance of CFH communication system can be expressed as

$$\mathrm{C}=\mathrm{C}_0+\mathrm{C}_1, \quad (6)$$

where C_1 is additional anti-interference gain by introducing a cognitive module.

A. Bit Error Rate (BER) of Conventional FH System

Encoding, modulation, and demodulation methods all affect the BER performance of FH communication systems. Since the transmitter in the conventional FH communication system does not consider whether there is an interference signal in the transmission environment, it directly selects the frequency slots from the set of frequency slots to send information.

Obviously, when the conventional FH communication system has k frequency slots occupied by interference signals, the probability that the information transmits in the interfered frequency slots is

$$\mathrm{Pr}_{\mathrm{int1}} = \frac{k}{n}. \quad (7)$$

Therefore, the BER of FH communication system with interference signals is

$$P_{e1} = \frac{n-k}{n} F(\frac{S}{N}) + \frac{k}{n} F(\frac{S}{N+J}),\ (0 \leq k \leq n) \quad (8)$$

where $F(\cdot)$ indicates a BER function of the FH communication system when transmitting information in one frequency slot.

B. BER of CFH System

1) Without interference signal: If there is no interference signal in the CFH communication system, the BER of the system is the same as that of the conventional FH system, which can be given as

$$Q_{un} = F(\frac{S}{N}). \quad (9)$$

2) Interference signal exists without missed detection: When the frequency slots occupied by the interference information is completely perceived, that is, the CFH communication system has no missed detection. The CFH communication system can select the frequency slots without interference for transmitting the information through the spectrum sensing results, effectively avoiding all interference frequency slots. Therefore, the probability of interference detection is

$$\mathrm{Pr}_{no-miss} = (1 - P_{md})^k. \quad (10)$$

Consequently, under the condition that the CFH communication system has interference and no missing detection, the BER of this system is

$$Q_1 = (1 - P_{md})^k F(\frac{S}{N}). \quad (11)$$

3) Interference signal exists with missed detection: However, when the frequency slots occupied by the interference signals are not fully perceived, there is a miss detection in CFH communication system. Although the CFH communication system can select the frequency slots without interference based on the results of spectrum sensing, the frequency slots used to transmit information may still occupy the interfered frequency slots due to incorrect sensing results. Therefore, the influence of interference signals on the transmission process is inevitable. Accordingly, for CFH systems, the number of frequency slots occupied by interference signal is

$$k^* = k - i + j, \quad (12)$$

where i $(0 < i < n)$ indicates the number of miss detection of the frequency slots occupied by the interference signal, j $(0 < j < n)$ represents the number of false alarms, and the number of i and j are independent of each other. Furthermore, the number of frequency slots without interference signal is

$$n - k^* = n - k + i - j. \tag{13}$$

Therefore, when there is a missed detection and false alarm in the spectrum sensing results of the interference signals, the probability of the interference detection is

$$\mathrm{Pr}_{ij} = C_k^i P_{md}^i (1 - P_{md})^{k-i} C_{n-k}^j P_f^i (1 - P_f)^{n-k-j}, \tag{14}$$

where

$$C_k^i = \frac{k(k-1)\cdots(k-i+2)(k-i+1)}{i(i-1)(i-2)\cdots 2 \cdot 1}. \tag{15}$$

Under this condition, the probability of transmitting information in the interfered frequency slots is

$$\mathrm{Pr}_{\mathrm{int2}} = \sum_{i=1}^{k} \sum_{j=0}^{n-k} (P_{ij} \cdot \frac{i}{n-k^*}). \tag{16}$$

In contrast, the probability of transmitting information in the frequency slots without interference is

$$\mathrm{Pr}_{no-\mathrm{int2}} = \sum_{i=1}^{k} \sum_{j=0}^{n-k} (P_{ij} \cdot \frac{n-k^*-i}{n-k^*}). \tag{17}$$

Combined with (9), (16) and (17), the BER of the CFH communication system with the missed detection and interference signals is

$$Q_2 = \sum_{i=1}^{k} \sum_{j=0}^{n-k} P_{ij} (\frac{i}{n-k^*} \cdot F(\frac{S}{N}) + \frac{n-k^*-i}{n-k^*} F(\frac{S}{N+J})). \tag{18}$$

Considering Section III-B2 and Section III-B3, the BER of CFH communication system with the interference signals can be concluded as

$$\begin{aligned} Q &= Q_1 + Q_2 \\ &= \sum_{i=1}^{k} \sum_{j=0}^{n-k} P_{ij} \left(\tfrac{n-k^*-i}{n-k^*} F(\frac{S}{N+J}) + \frac{i}{n-k^*} \cdot F(\frac{S}{N}) \right) \\ &+ F(\frac{S}{N}) \cdot (1 - P_{md})^k \\ &= \sum_{i=1}^{k} \sum_{j=0}^{n-k} P_{ij} \left(\frac{(n-k-j)F(\frac{S}{N+J}) + iF(\frac{S}{N})}{n-k+i-j} \right) \\ &+ (1 - P_{md})^k F(\frac{S}{N}). \end{aligned} \tag{19}$$

Consequently, considering the two factors of false alarm and missed detection, the BER of the CFH communication system is

$$P_2 = \begin{cases} F(\frac{S}{N}) & k = 0, \\ (1 - P_{md})^k F(\frac{S}{N}) + \sum_{i=1}^{k} \sum_{j=0}^{n-k} P_{ij} & \\ \cdot \left(\frac{iF(\frac{S}{N}) + (n-k-j)F(\frac{S}{N+J})}{n-k+i-j} \right) & k \neq 0. \end{cases} \tag{20}$$

4) Communication links convergence delay: The CFH communication system has no cognitive ability before the communication link converges. At this time, the BER of the CFH communication system is equal to the BER of the FH communication system. Once the communication links converge, the cognitive unit of the communication system begin to sense, analyze, and make decisions to generate frequency sets and communication scheme that can be used by the FH system. In addition, it is necessary to make this information pass through a highly reliable channel in time to achieve the synchronization of the FH frequency and the adjustment of the communication scheme at both ends of the transmitter and the receiver. Accordingly, the cognitive capability can be achieved in CFH communication systems. It is assumed thatT_L is the period of interference change, and T_s $(T_L > T_s)$ is the link convergence time. It should be noted that T_s includes interference sensing time, the time required for transmitting sense information and adjusting the FH transmission scheme. Therefore, considering the effect of link convergence time, the BER of the CFH communication system is

$$P_e = \frac{T_s}{T_L} P_1 + \frac{T_L - T_s}{T_L} P_2. \tag{21}$$

Therefore, cognitive anti-interference gain can be expressed as

$$\mathrm{C}_1 {=} F^{-1}(P_e) - F^{-1}(P_1), \tag{22}$$

where the system function $F^{-1}(\cdot)$ is the inverse of the BER function $F(\cdot)$. And the reliability tolerance of CFH communication system can be rewritten as

$$\mathrm{C} {=} \mathrm{C}_0 + \mathrm{F}^{-1}(\mathrm{P}_\mathrm{e}) - \mathrm{F}^{-1}(\mathrm{P}_1). \tag{23}$$

IV. Numerical Results

This section presents the simulation results to evaluate the reliability tolerance of the CFH communication system. In our simulation, the frequency range used by the CFH communication system tested is from 2.65 GHz to 2.95 GHz. In addition, the occupied bandwidth W is 300 MHz and the frequency hopping slots n is 60. That is, the bandwidth occupied by each frequency slot is $B = 5$ MHz. Additionally, the signal-to-noise ratio ranges from 0 to $12dB$. Here, the signal-to-noise ratio (S/N) is converted to a normalized signal-to-noise ratio ($\mathrm{E_b/N_0}$). Moreover, the false alarm probability P_f is assumed to be 0.1. The number of frequency slots occupied by the interference signals is $k = 30$.

When the probability of missed detection P_{md} is 0.1 and the interference power I is -28 dBw, Fig. 3 intuitively reflects

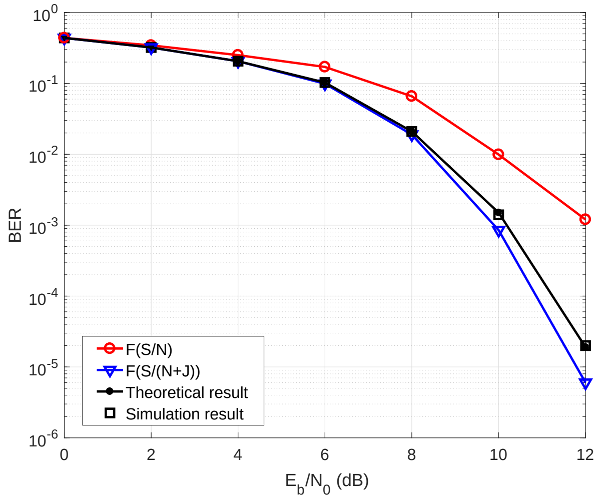

Fig. 3. BER performance of three different types of FH communication systems with $P_{md} = 0.1$ and $I = -28$ dBw.

the change of the BER performance of the CFH system, the conventional FH system without interference and the FH system with interference as the signal-to-noise ratio (SNR). It can be seen from the Fig. 3 that the simulation results of BER performance can be consistent with the theoretical results, which proves the rationality of the proposed reliability tolerance measurement method. Moreover, as the normalized signal-to-noise ratio increase, the BER performance decreases gradually. This shows that with a certain background noise power, as the transmission power increase, the possibility for authorized user to receive complete information increases rapidly. We can also find that under the same signal-to-noise ratio, the performance curve of the CFH system is between the simulation curves of the other two systems, which proves that this CFH system can effectively resist the threat of interference signals.

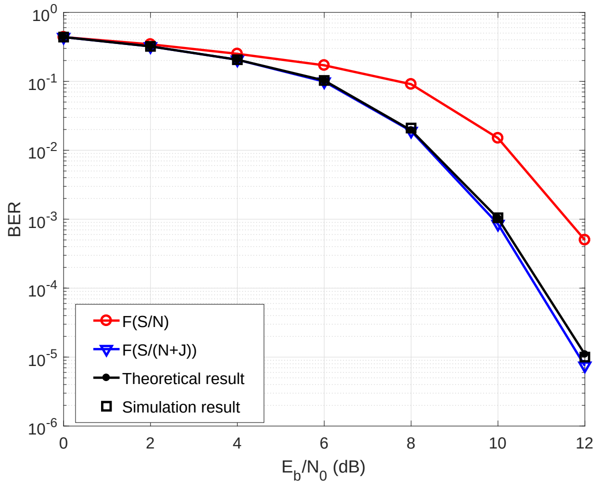

Fig. 4. BER performance of three different types of FH communication systems with $P_{md} = 0.01$ and $I = -32$ dBw.

Different from the Fig. 3, Fig. 4 reflects the BER performance curves when the probability of missed detection P_{md} is 0.01 and the interference power I is -32 dBw. By comparing the simulation results of the interference signal on the BER performance of the FH system in Fig. 3 and Fig. 4, it can be found that the reliability performance of the system decreases gradually as the increase of interference power. However, since the CFH communication system can acquire the channel conditions and update the frequency hopping sequence in time through the spectrum sensing method, the CFH system can effectively guarantee its reliability performance. At the same time, it also reflects that the reliability performance of the cognitive system is enhanced with the increase of the power of the interference signal.

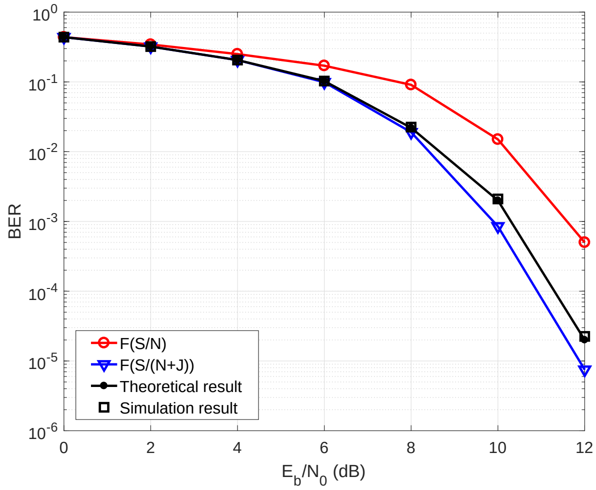

Fig. 5. BER performance of three different types of FH communication systems with $P_{md} = 0.01$, $T_L = T_s/5$, and $I = -32$ dBw.

On the basis of analyzing the influence of false alarm probability and missed detection probability on interference tolerance, Fig. 5 adds another consideration to the key factor of communication links convergence delay, which is a factor that cannot be ignored in the actual communication environment. It can be seen that the BER performance of the CFH system has decreased. This is due to the fact that the cognitive system's perception of interference signals, the transmission of sensing results, and the adjustment of FH sequences, which all cause time delays. Note that, it is still possible to ensure that the anti-interference gain of the CFH communication system is stable at 1.3 dB or more when the BER is 10^{-3}.

V. Conclusion

Based on the lack of analysis for the reliability performance of the CFH communication system in the existing literature, this paper proposes an analysis method that can effectively measure the reliability tolerance of the system. We first have proposed a transmission scheme of the CFH, and then by analyzing the influences of false alarm probability, missed detection probability, and communication link convergence delay, an analytical expression of reliability tolerance has been derived. Simulation results reflect that this method can effectively measure the reliability of CFH communication systems, and provide a useful reference for studying complex and practical FH communication systems. In future work, based on the above theoretical derivation, the reliability of CFH systems can be optimized by adjusting relevant parameters to meet different requests.

Acknowledgment

Research and development leading to these results are funded by the National Natural Science Foundation for Distinguished Young Scholar 61825104, by the Key project of National Natural Science Foundation of China 61631015, by the National Natural Science Foundation of China 61501354, 61501356, 61901328, by University Innovation Platform Project 2019921815KYPT009JC011, and by China Postdoctoral Science Foundation 2019M653558.

References

[1] A. Attar, H. Tang, A. V. Vasilakos, and F. R. Yu, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172-3186, Dec. 2012.

[2] R. D. Pietro and G. Oligeri, "Jamming mitigation in cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 10-15, Jun. 2013.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.

[4] C. Li, Z. Li, J. Shi, L. Guan, and L. Zhang, "Intelligent spectrum control in heterogeneous networks with high security capability," *IEEE Wireless Commun. Lett.*, Early Access, Feb. 2020. doi: 10.1109/LWC.2020.2972272.

[5] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A suvery on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 428-445, 1st Quart. 2013.

[6] L. Zhang, G. Ding, Q. Wu, *et al.*, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342-1363, Apr. 2015.

[7] H. Jagadeesh and Y. Hu, "Convolution Attack on Frequency Hopping by Full-Duplex Radios," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5642-5656, June 2019.

[8] Z. Chen, H. Li, G. Cui, and M. Rangaswamy, "Adaptive transmit and receive beamforming for interference mitigation," *IEEE Signal Process. Lett.*, vol. 21, no. 2, pp. 235-239, Feb. 2014.

[9] Z. Yang and M. Dong, "Low-complexity coordinated relay beamforming design for multi-cluster relay interference networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2215-2228, Apr. 2019.

[10] W. Liu, K. Huang, X. Zhou, and S. Durrani, "Full-duplex backscatter interference networks based on time-hopping spread spectrum," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4361-4377, July 2017.

[11] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE J. Sel. Area Commun.*, vol. 28, no. 5, pp. 703 -715, June 2010.

[12] L. Guan, Z. Li, J. Si, and R. Gao, "Generation and characteristics analysis of cognitive-based high-performance wide-gap FH sequences," *IEEE Trans. Veh. Technol.*, vol. 64, no. 11, pp. 5056-5069, Nov. 2015.

[13] H. Cai, Y. Yang, Z. Zhou, and X. Tang, "Strictly optimal frequency-hopping sequence sets with optimal family sizes," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 1087-1093, Feb. 2016.

[14] W. Chen, G. Yang, M. Chang, and W. Kwong, "Construction and analysis of shift-invariant, asynchronous-symmetric channel-hopping sequences for cognitive radio networks," *IEEE Trans. Commun.*, vol. 65, no. 4, pp. 1494-1506, Apr. 2017.

[15] L. Guan, Z. Li, B. Hao, J. Si, and B. Ning, "Cognitive Frequency Hopping Sequences," *Chinese Journal of Electronics*, vol. 25, no. 1, pp. 185-191, Jan. 2016.

[16] Z. Zhou, X. Tang, D. Peng, and U. Parampalli, "New constructions for optimal sets of frequency-hopping sequences," *IEEE Trans. Inf. Technol.*, vol. 57, no.6, pp. 3831-3840, Jun. 2011.

[17] M. Amjad, F. Akhtar, M. H. Rehmani, *et al.*, "Full-duplex communication in cognitive radio networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 19, no. 4, pp. 2158-2191, Jun. 2017.

[18] D. Wang, N. Zhang, Z. Li, F. Gao, and X. Shen, "Leveraging high order cumulants for spectrum sensing and power recognition in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1298-1310, Feb. 2018.