Effects of Shadow Fading on Energy Detection and Matched Filter Detection in Cognitive Radio Network

Hong Du[1], Dacheng Wang[2], and Long Chen[1]
(Corresponding author: Dacheng Wang)

School of Electrical and Engineering, Chongqing University of Technology[1]
Institute of Science and Technology, Chongqing University of Technology[2]
No. 69, Hongguang Avenue, Banan District, Chongqing, China. 400054
Email: wdc@cqut.edu.cn

(Received Nov. 20, 2022; Revised and Accepted June 30, 2023; First Online July 10, 2023)

Abstract

Spectrum sensing can improve the spectrum's utilization using licensed spectrum in cognitive radio. However, various security issues, such as malicious user attacks and shadow fading, affect network performance. This study focuses on how energy and matched filter detection in cognitive radio are affected by shadow fading. The formulas for the probability of detection and false alarm are derived for energy and matched filter detection, respectively. According to the simulation, matched filter detection is more susceptible to shadow fading than energy detection in an environment with a lower signal-to-noise ratio.

Keywords: Cognitive Radio; Energy Detection; Matched Filter Detection; Shadow Fading; Spectrum Sensing

1 Introduction

The Federal Communications Commission (FCC) is considering opening a portion of the authorized spectrum to unauthorized users without interfering with authorized primary users (PUs) because the allocation of fixed spectrum is no longer sufficient to meet the requirements of an increasing number of users due to the rapid development of wireless communication. With the development of cognitive radio (CR), it is now possible to use the authorized free frequency band without interfering with the primary user. Therefore, the utilization of spectrum resources is improved, and the spectrum requirements of a more significant number of wireless users are met, which is an important technology to address the problem of a lack of resources in wireless spectrum resources [23]. Cognitive radio networks are wireless communication networks with cognitive characteristics. The network can observe the surrounding wireless network environment, use environmental cognition to get information about how spectrum is used, process and learn the information, make intelligent decisions and analyses, dynamically access the available spectrum, and finally adapt and reconfigure itself to adapt to the cognitive radio network environment, which is constantly changing, to achieve optimal network performance.

A cognitive radio user is a user in a cognitive radio network, and the primary user is the cognitive radio user's counterpart. The CR user accesses to communicate when the PU is not using the channel. Once the signal of the PU returns, the CR user immediately withdraws from the channel it is communicating on and looks for other available free channels to communicate. Therefore, the CR user should first have the spectrum sensing function to detect the signal from the wireless environment, then determine the spectrum hole after analysis and adjustment, and use the spectrum hole to communicate without affecting the PU. Spectrum sensing technology, a prerequisite for operating cognitive radio networks, means that CR users collect spectrum usage information in wireless networks via various signal detection and processing methods to find spectrum holes.

Cognitive radio technology aims to solve the spectrum scarcity issue by implementing dynamic spectrum management. However, various security issues and vulnerabilities experienced can influence network performance [22]. Authors in [6] have investigated robust spectrum sensing schemes against malicious user attacks. In cognitive networks, many denial-of-service attacks will cause significant performance degradation and thus need to be detected quickly [12,14,18]. An algorithm to reduce the detection delay is presented in [21] so that a network manager can respond to an event as quickly as possible to minimize the impact of attacks.

Additionally, the structure of the cognitive radio network introduced a spectrum sensing data falsification (SSDF) attack. In such attacks, malicious users make incorrect observations of the system's fusion center, which may cause licensed users to experience the severe quality of service degradation and disruption. The authors of [13] investigate the threat and the mitigation strategy for SSDF attacks. The Byzantine attack is one of the key issues preventing the success of cognitive radio sensor networks. The Byzantines can be avoided using the security measures suggested in [2]. A reliable sensing method has been developed to prevent the Byzantine attack. Additionally, CR users naturally face two significant security threats: jamming and primary user emulation (PUE) attacks. Machine learning has been applied to detect these attacks in [15]. The proposed deep learning-assisted detection method performs exceptionally well when spotting these threats.

Shadowing also limits the effectiveness of spectrum-sensing techniques in cognitive radio in [3, 20]. S. Kavaiya in [10] examined how an improved energy detector performs over uniformly and exponentially correlated Nakagami-m fading with imperfect channel state information (CSI). Simulation results show that user mobility and correlated fading combined affect the detection performance over imperfect CSI. In addition, H. Rasheed in [16] quantifies energy detection for spectrum sensing under shadowed conditions. A study in [5] examines performance analysis of cooperative spectrum sensing over shadowed fading. H. Huang in [9] discuss the unified performance of energy detection of spectrum sensing over generalized fading channels in cognitive radios. Fading channels will undoubtedly impact the detection performance of spectrum sensing. The results demonstrate that fading channels will impact energy detection performance, but that sensing performance can be enhanced using the appropriate channel parameters. Aulakh in [1] shows the solutions to shadow fading using two strong techniques: optimal spectrum sensing and greedy spectrum sensing. The authors of [8, 19] also investigated the sensing performance for cooperative spectrum sensing in fading channels.

The rest of the paper is organized as follows: Sections 2 and 3 looked at the spectrum sensing system model for energy and matched filter detection. Additionally, the effect of shadow fading on detection performance is discussed. Section 4 presented the simulation results and discussed the influence on the detection performance. Finally, Section 5 contains the conclusions.

2 Energy-Detection Based Spectrum Sensing Technology

Energy detection is the most commonly used method in spectrum sensing due to its simplicity. An energy detector can determine whether signals are present in a particular frequency band by detecting received signals. The steps involved in detecting energy are shown in Figure 1 as follows. After passing through an ideal Band Pass Filter (BPF), the received signal calculates the energy of signals in the band in the detecting time T, which is then compared to the threshold to determine if communications use the frequency band.

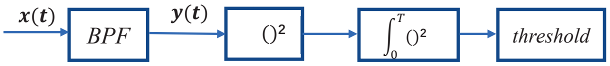

Figure 1: Block diagram of energy detection

Two presumptions can be made for spectrum sensing. H_0 denotes no primary user signal in a certain spectrum band as in Equation (1). H_1 means that a primary user signal exists in that band as in Equation (2).

$$H_0 : y(t) = n(t) \tag{1}$$

$$H_1 : y(t) = h(t)s(t) + n(t) \tag{2}$$

y(t) is the received signal by the CR user at time t. $n(t)$ is the Additive White Gaussian Noise (AWGN). We assume that $n(t)$ has a variance of 1 and an expectation of 0 under a standard normal distribution. $s(t)$ is the primary user's transmitting signal. h is the channel coefficient.

In energy detection, the sampling time is T, the signal bandwidth is W, and the number of sampling points is $N = 2TW$. It is assumed that the decision threshold is K, the signal-to-noise ratio is $\lambda_0 = \frac{E_s}{N_0}$. The detection probability, false alarm probability, and missed detection probability are shown as in Equation (3), in Equation (4) and in Equation (5):

$$P_{fa} = Q(\frac{K-N}{\sqrt{2N}}) = \frac{1}{2}erfc(\frac{K-N}{\sqrt{4N}}) \tag{3}$$

$$P_d = Q(\frac{K-N-N\lambda_0}{\sqrt{2N+N\lambda_0}}) = \frac{1}{2}erfc(\frac{K-N-N\lambda_0}{\sqrt{4N+2N\lambda_0}}) \tag{4}$$

$$P_{md} = 1 - P_d \tag{5}$$

Shadow fading will impact the primary user's signal during transmission. The normal log component of the shadow loss and the m power of the wave propagation distance r is typically used to calculate shadow fading. Here, we consider the impact of shadow loss. ζ is the log loss (in dB) caused by shadow, which follows a lognormal distribution with zero mean and variance of 1dB.

The probability of false alarm and the probability of detection can be expressed by as in Equation (6) and in Equation (7).

$$P_{fa} = \frac{1}{2}erfc(\frac{K-N}{\sqrt{4N}}) \tag{6}$$

$$P_d = \frac{1}{2}erfc(\frac{K-N-N\lambda_2}{\sqrt{4N+2N\lambda_2}}) \tag{7}$$

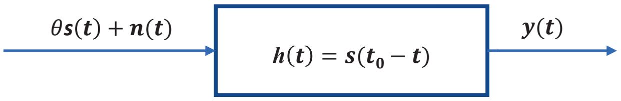

Figure 2: Block diagram of matched filter detection

3 Matched Filter Based Spectrum Sensing Technology

Matching filter detection necessitates prior knowledge of the primary user signal's modulation method, pulse waveform, timing, and packet format, among other things [4, 7, 11, 17]. We presume that BPSK is being used as a modulator in this case. The block diagram is displayed in Figure 2. The noise signal $n(t)$ satisfies the Gaussian distribution, and $\theta = 1$ indicates the primary user's presence, while $\theta = 0$ indicates its absence.

$y(t)$ is the received signal by the CR user which can be expressed by as in Equation (8)

$$y(t) = \int_0^t [\theta s(\tau) + n(\tau)]h(t - \tau)d\tau \tag{8}$$

When $t = t_0$, the CR user receives the signal. When the primary user's signal exists H_1, $s_1 = s(t) + n(t)$, then

$$y(t_0) = \int_0^{t_0} [s(\tau) + n(\tau)]s(\tau)d\tau = E_1 + Z \tag{9}$$

The received signal's probability distribution is given as in Equation (10):

$$p(y|s_1) = \frac{1}{\sqrt{\pi N_0 E_1}} exp[-\frac{(y - E_1)^2}{N_0 E_1}] \tag{10}$$

When the primary user's signal does not exist H_0, $s_2 = n(t)$, then

$$y(t_0) = \int_0^{t_0} n(\tau)s(\tau)d\tau = Z \tag{11}$$

The probability distribution of the received signal is expressed as in Equation (12):

$$p(y|s_2) = \frac{1}{\sqrt{\pi N_0 E_1}} exp[-\frac{y^2}{N_0 E_1}] \tag{12}$$

Define the judgment threshold as V . The probabilities of false alarm, detection, and missed detection can be expressed as follows:

$$P_{fa} = p(y > V|H_0) = \frac{1}{2}erfc(\frac{V}{E_1}\sqrt{\frac{E_1}{N_0}}) \tag{13}$$

$$P_d = p(y > V|H_1) = 1 - \frac{1}{2}erfc(\sqrt{\frac{E_1}{N_0}} - \frac{V}{E_1}\sqrt{\frac{E_1}{N_0}}) \tag{14}$$

$$P_{md} = p(y < V|H_1) = \frac{1}{2}erfc(\frac{E_1 - V}{\sqrt{N_0 E_1}}) \tag{15}$$

The effect of shadowing loss ζ is also taken into account here. When $E_2 = E_1 10^{\frac{\zeta}{10}}$, the probabilities of false alarm and detection for matched filter detection can be expressed as in Equation (16) and Equation (17):

$$P_{fa} = \frac{1}{2}erfc(\frac{V}{E_2}\sqrt{\frac{E_2}{N_0}}) \tag{16}$$

$$P_d = 1 - \frac{1}{2}erfc(\sqrt{\frac{E_2}{N_0}} - \frac{V}{E_2}\sqrt{\frac{E_2}{N_0}}) \tag{17}$$

4 Simulation and Discussion

The influence on the detection performance from the probability of false alarm and shadow fading is simulated and discussed in energy and matched filter detection, respectively. The sampling point is N=1024.

4.1 Influence on Detection Performance from the Probability of False Alarm

Figure 3 shows that when the number of sampling point N is selected, the higher the probability a false alarm, the higher the probability of detection, and the lower the probability of missed detection.

In matched filter detection, the effect of the false alarm probability on the detection performance is depicted in Figure 4. It is evident that the higher the signal-to-noise ratio, the greater the probability of detection, and the lower the possibility of missed detection, the greater the probability of a false alarm. This is because when the false alarm probability is increased, equivalent to a lower limit on the system, the probability of missed detection will be reduced accordingly.

It can also be seen that the threshold has the same increasing and decreasing properties for the probability of detection and false alarm. The higher the probability of a false alarm, the higher the probability of detection, and the lower the probability of missed detection when the signal-to-noise ratio is calculated. The higher the signal-to-noise ratio, on the assumption that the probability of a false alarm is calculated, the greater the probability of detection.

4.2 Influence on Detection Performance from Shadow Fading

The following simulations examine how shadow fading affects the performance of energy detection and matched filter detection, respectively, under the assumption that the probability of false alarm is 0.01.

According to Figure 5, the probability of detection affected by shadow fading is lower than the probability of detection without shadow fading for the same probability of a false alarm; The probability of missed detection when

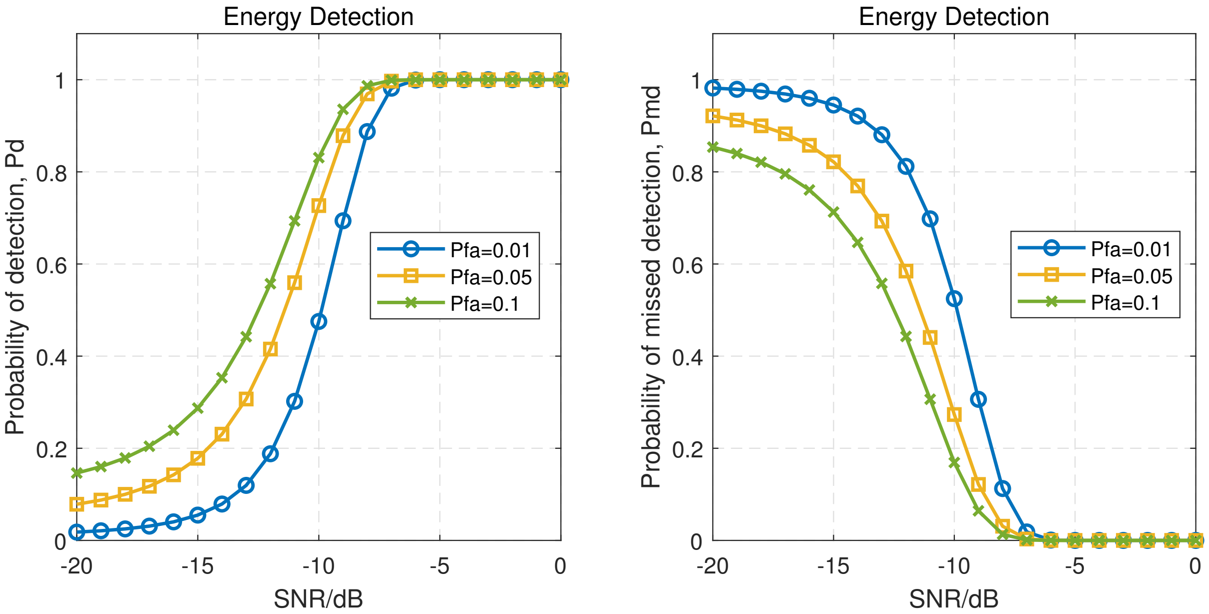

Figure 3: Influence on detection performance from different probability of false alarm in energy detection

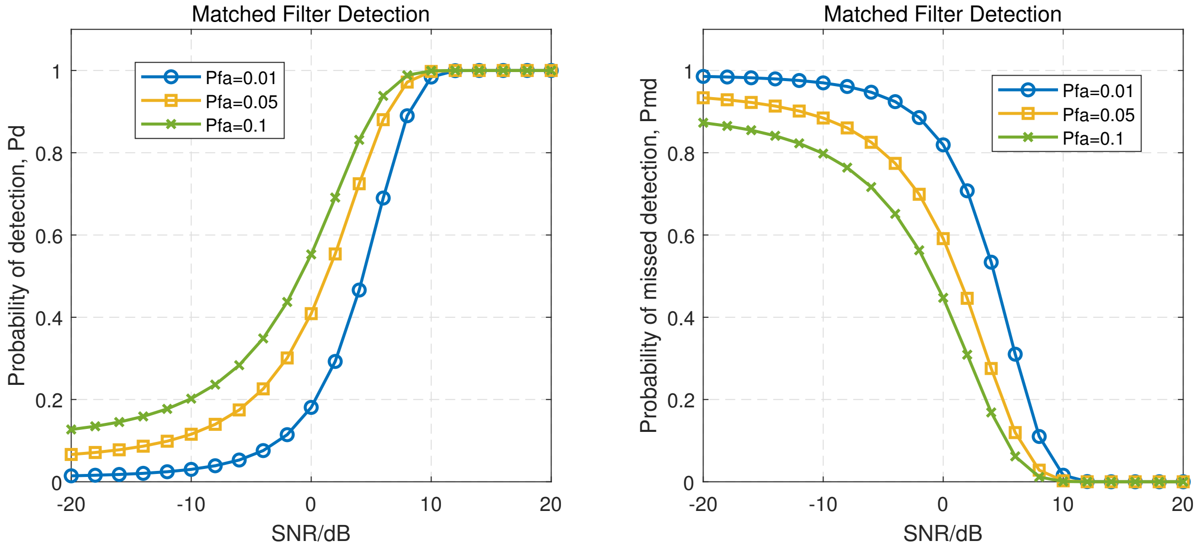

Figure 4: Influence on detection performance from false alarm probability in Matched Filter detection

shadow fading is present is greater than the probability of missed detection when shadow fading is not present. Other approaches (like the multi-node cooperative detection algorithm) are required to reduce since shadow fading impacts detection performance significantly.

According to Figure 6, the probability of detection affected by shadow fading is lower than that of detection without shadow fading for the same probability of a false alarm. In comparison, the probability of missed detection affected by shadow fading is higher than that of missed detection without shadow fading. The impact of shadow fading on detection performance is very large, so other methods, such as the multi-node cooperative detection method, are needed to overcome the impact of shadow fading.

Table 1 displays the comparison study for the energy and matched filter detection under various shadow fading when the SNR=-10dB. As seen, matched filter detection's sensing performance is more susceptible to shadow fading than energy detection.

5 Conclusions

Cognitive radio aims to solve the spectrum scarcity issue by implementing spectrum sensing technology. In fact, various security issues and vulnerabilities experienced can influence network performance, such as malicious user attacks and shadow fading. Shadow fading's effects on energy detection and matching filter detection are examined in this research. The formulas for detection probability and false alarm probability are constructed for the energy detection and matching filter detection technologies. The probability of detection and missed detection under different false alarm probabilities and shadow fading is simulated and discussed, respectively. Shadow fading has a more significant impact on matched filter detection than energy detection, as the simulation results show.

Acknowledgments

This work was supported by the Science and Technology Research Program of Chongqing Municipal Education Commission (Grant No. KJQN202101123, KJQN202101110, KJQN202101128). This work was supported by 2021 Chongqing Doctoral Through Train scientific research project (No.CSTB2022BSXM-JCX0118, (No.CSTB2022BSXM-JCX0119). This work was supported by scientific research start-up fund project of Chongqing University of Technology (No.2020ZDZ013) (No.2022ZDZ013).

References

[1] I. K. Aulakh and N. Kaur, "Optimal sensing simulation in crns under shadow-fading environments," in *3rd International Conference on Computing for Sustainable Global Development (INDIACom'16)*, pp. 901–905, 2016.

[2] M. A. Aygül, H. M. Furqan, M. Nazzal, and H. Arslan, "Deep learning-assisted detection of pue and jamming attacks in cognitive radio systems," in *IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, pp. 1–5, 2020.

[3] D. Bera, I. Chakrabarti, S. S. Pathak, and G. K. Karagiannidis, "Another look in the analysis of cooperative spectrum sensing over nakagami- m fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 856–871, 2017.

[4] A. Brito, P. Sebastião, and F. J. Velez, "Hybrid matched filter detection spectrum sensing," *IEEE Access*, vol. 9, pp. 165 504–165 516, 2021.

[5] G. Chandrasekaran and S. Kalyani, "Performance analysis of cooperative spectrum sensing over $\kappa-\mu$ shadowed fading," *IEEE Wireless Communications Letters*, vol. 4, no. 5, pp. 553–556, 2015.

[6] J. C. Clement and K. C. Sriharipriya, "Robust spectrum sensing scheme against malicious users attack in a cognitive radio network," in *International Conference on Electrical, Computer and Energy Technologies (ICECET'21)*, pp. 1–4, 2021.

[7] S. Dhananjaya and B. N. Yuvaraju, "A novel method in matched filter spectrum sensing to minimize interference from compromised secondary users of cognitive radio networks," in *International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT'18)*, pp. 228–231, 2018.

[8] H. Guo, N. Reisi, W. Jiang, and W. Luo, "Soft combination for cooperative spectrum sensing in fading channels," *IEEE Access*, vol. 5, pp. 975–986, 2017.

[9] H. Huang and C. Yuan, "Cooperative spectrum sensing over generalized fading channels based on energy detection," *China Communications*, vol. 15, no. 5, pp. 128–137, 2018.

[10] S. Kavaiya and D. K. Patel, "On the performance of an improved energy detector over shadow fading channels for vehicular networks," in *14th International Conference on COMmunication Systems and NETworkS (COMSNETS'22)*, pp. 275–279, 2022.

[11] R. T. Khan, S. Zaman, M. I. Islam, and M. R. Amin, "Performance evaluation of cognitive radio network under matched filter detection," in *International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC'17)*, pp. 1196–1201, 2017.

[12] M. Lebepe and M. Velempini, "Mitigation of denial of service attacks in software-defined cognitive radio networks," in *International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD'21)*, pp. 1–5, 2021.

[13] M. Y. Morozov, O. Y. Perfilov, N. V. Malyavina, R. V. Teryokhin, and I. Chernova, "Combined approach to ssdf-attacks mitigation in cognitive radio networks," in *Systems of Signals Generating and*

Table 1: The probability of detection with the different shadow fading. (SNR=-10dB)

shadow fading	**Pd of energy detection**	**Pd of matched filter detection**
0	0.83	0.03
-1	0.72	0.02
-5	0.26	0.01
-10	0.15	0.007

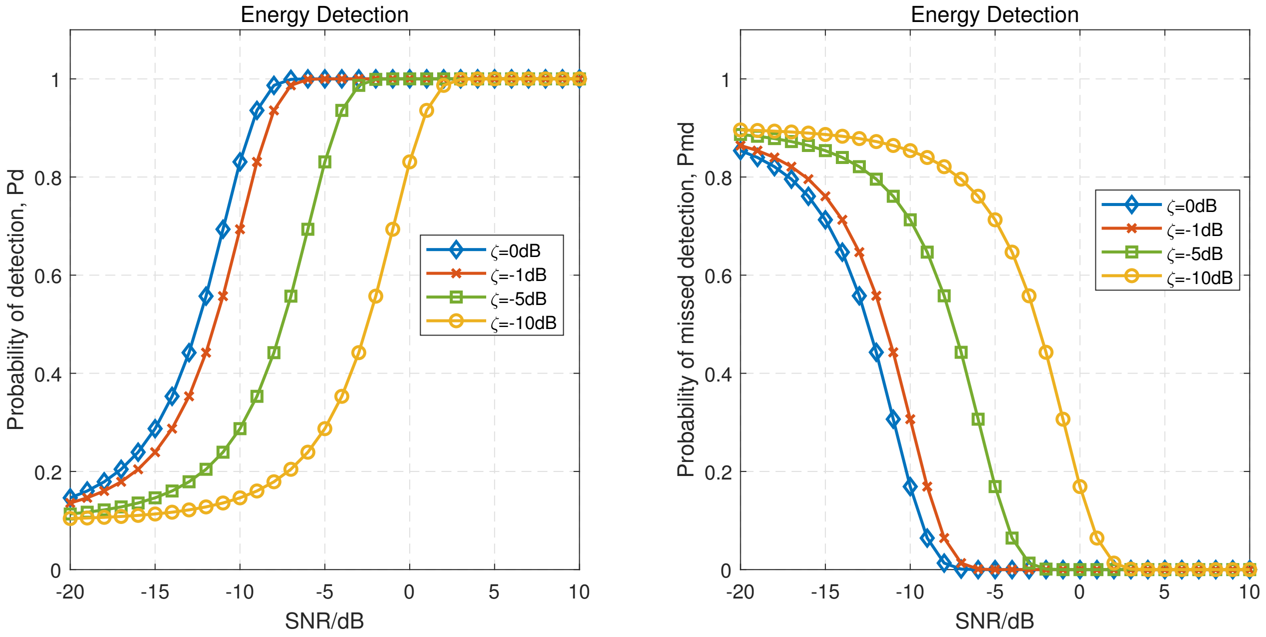

Figure 5: Influence on detection performance from the different shadow fading in energy detection

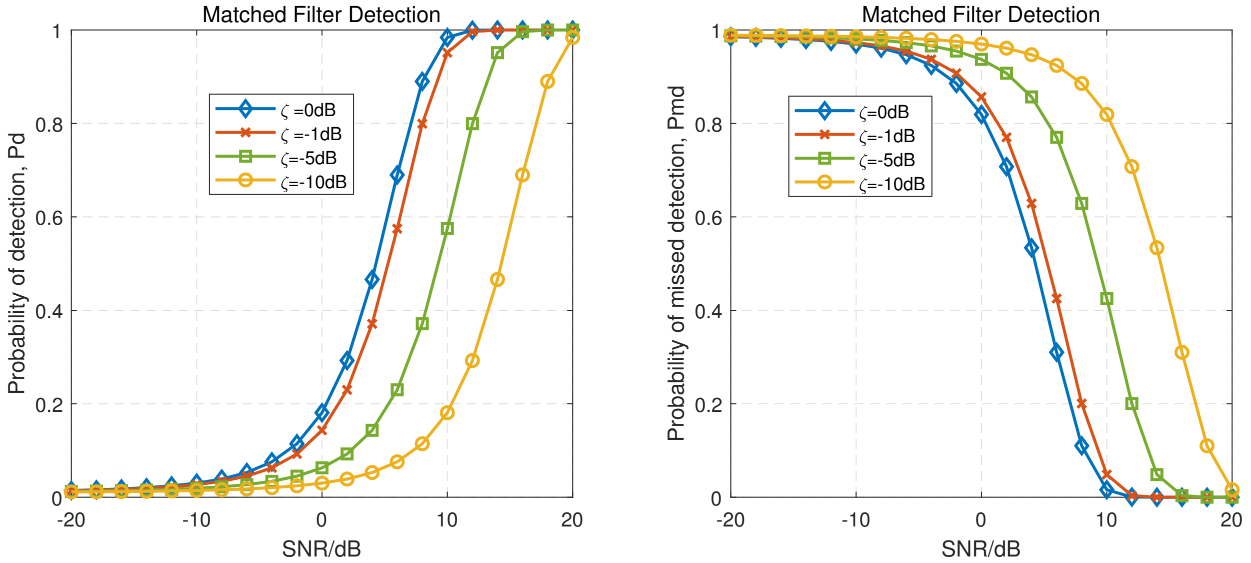

Figure 6: Influence on detection performance from the different shadow fading in Matched Filter detection

Processing in the Field of on Board Communications, pp. 1–4, 2020.

[14] N. P. Mwanza and J. Kalita, "Detecting ddos attacks in sdn using deep learning techniques: A survey," *International Journal of Network Security*, vol. 25, no. 2, pp. 360–376, 2023.

[15] S. R. Patil, R. Rajashree, and J. Agarkhed, "A survey on byzantine attack using secure cooperative spectrum sensing in cognitive radio sensor network," in *6th International Conference on Computing Methodologies and Communication (ICCMC'22)*, pp. 267–270, 2022.

[16] H. Rasheed, N. Rajatheva, and F. Haroon, "Spectrum sensing with energy detection under shadow-fading condition," in *IEEE 5th International Symposium on Wireless Pervasive Computing*, pp. 104–109, 2010.

[17] N. Reddy, P. S. Poojitha, M. Kumar, and K. Ramya, "Reducing the sensing errors by adopting the effective matched filter threshold estimation in lower snr conditions," in *International Conference on Emerging Trends in Science and Engineering (ICESE'19)*, vol. 1, pp. 1–4, 2019.

[18] S. Sedaghat, "The forensics of ddos attacks in the fifth generation mobile networks based on software-defined networks," *International Journal of Network Security*, vol. 22, no. 1, pp. 41–53, 2020.

[19] G. Sharma and R. Sharma, "Distributed cooperative spectrum sensing over different fading channels in cognitive radio," in *International Conference on Computer, Communications and Electronics (Comptelix'17)*, pp. 107–111, 2017.

[20] P. C. Sofotasios, A. Bagheri, T. A. Tsiftsis, S. Freear, A. Shahzadi, and M. Valkama, "A comprehensive framework for spectrum sensing in non-linear and generalized fading conditions," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 8615–8631, 2017.

[21] C. Sorrells and L. Qian, "Quickest detection of denial-of-service attacks in cognitive wireless networks," *International Journal of Network Security*, vol. 16, no. 6, pp. 468–476, 2014.

[22] K. Sudha, K. A. Kumari, and D. Varunika, "A critical survey on security issues in cognitive radio networks," in *International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS'23)*, pp. 292–297, 2023.

[23] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

Biography

Hong Du is a Lecturer/ Master supervisor in Chongqing University of Technology, she received PhD from Beijing University of Post and Technology in 2012 and worked at School of Electrical and Engineering in Chongqing University of Technology. Her research interests include cognitive network and information security.

Dacheng Wang is a Senior Engineer, he received PhD from Northeast Petroleum University in 2021, and now worked in Chongqing University of Technology. His research interests include network and information security.

Long Chen is a Lecturer, he received PhD from Chongqing University in 2018, and then worked at School of Electrical and Engineering in Chongqing University of Technology. His research interests include network and information security, wireless communication technology.