https://dx.doi.org/10.4314/dujopas.v10i3b.32
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 10 No. 3b September 2024*

Jamming and Anti-Jamming Solutions for 5G and IoT

F.O Aghware,[1*] **J.O Ogala**[2]

[1]Department of Computer Science,
University of Delta, Agbor.

[2]Department of Cyber Security,
University of Delta, Agbor

Email: fidelis.aghware@unidel.edu.ng

Abstract

Wireless networks, especially 5G and IoT networks, are vulnerable to intentional interference or jamming. Jamming attacks can cause severe disruption to network operations and compromise the confidentiality and integrity of transmitted data. Therefore, effective anti-jamming techniques are essential for ensuring the reliability and security of these networks. This paper presents a comprehensive survey of state-of-the-art anti-jamming solutions for 5G and IoT networks. The paper covers the different types of jamming attacks, their impact on network performance, and the various anti-jamming techniques such as frequency hopping, spread spectrum techniques, beamforming, multi-antenna systems, and physical layer security. The paper also includes an experimental evaluation of anti-jamming techniques and provides practical implications and recommendations. The findings of this study can help network engineers and researchers to design more secure and resilient wireless networks in the 5G and IoT era.

Keywords: jamming, anti-jamming, 5G, IoT, wireless networks

INTRODUCTION

The proliferation of 5G and IoT technologies has revolutionized the way we communicate and interact with our environment, enabling a wide range of applications that provide users with unprecedented levels of connectivity, data throughput, and convenience. However, these technologies also bring about new security challenges, as they are vulnerable to various types of cyber-attacks, including jamming attacks. Jamming attacks involve the intentional interference with wireless signals, disrupting their transmission and reception, which can significantly degrade network performance and disrupt critical services in 5G and IoT networks (Zhang, 2022; Al-Fuqaha, 2015).

Jamming attacks can have severe consequences, ranging from disrupting communication services in smart cities, transportation systems, and industrial IoT deployments to compromising the safety and security of critical infrastructure. As such, there is a growing need for effective anti-jamming solutions that can protect 5G and IoT networks against these types of threats. While some anti-jamming techniques have been proposed, there is a lack of comprehensive evaluations and analyses of the current state-of-the-art solutions for 5G and IoT networks. Therefore, this study aims to review and analyze the existing anti-jamming solutions for 5G and IoT networks, including their strengths, weaknesses, and performance

Author for Correspondence

evaluations, to address this research gap and provide insights for the development of more effective and robust anti-jamming solutions in the future.

Jamming attacks are a serious threat to the security and reliability of 5G and IoT networks. According to (Zhang et al., 2020), jamming attacks can cause significant disruptions to wireless networks, rendering them unusable for critical applications such as emergency services, transportation, and healthcare. Moreover, jamming attacks can be easily launched using low-cost and readily available hardware, making them an attractive option for cyber criminals and malicious actors.

To address this threat, researchers and industry experts have been working on developing anti-jamming solutions that can detect and mitigate jamming attacks in real-time. For instance, (Lin et al., 2021) proposed a deep learning-based anti-jamming algorithm that can effectively mitigate jamming attacks in 5G networks. The creation and implementation of a machine learning-based anti-jamming system that can identify and mitigate jamming threats in IoT networks has been the subject of notable publications by traditional researchers. (Han, et al., 2020), (Wu, et al., 2022), (Yang et al., 2020), (Lin et al., 2024).

The main objective of this study is to review and analyze the current state-of-the-art anti-jamming solutions for 5G and IoT networks. Specifically, this study aims to:

1. Provide an overview of the different types of jamming attacks that can affect 5G and IoT networks
2. Review the existing anti-jamming solutions for 5G and IoT networks, including their strengths and weaknesses
3. Evaluate the performance of selected anti-jamming solutions using experimental simulations and real-world datasets
4. Identify the key challenges and future research directions in the field of anti-jamming for 5G and IoT networks.

To achieve these objectives, this study will review and analyze the relevant literature, including academic papers, technical reports, and industry publications. The study will also conduct experiments using simulation tools and real-world datasets to evaluate the performance of selected anti-jamming solutions. By providing a comprehensive overview of the current state-of-the-art in anti-jamming solutions for 5G and IoT networks, this study can help inform the development of more effective and robust anti-jamming solutions in the future.

The research gap that this study intends to fill is the lack of a comprehensive overview and evaluation of the current state-of-the-art anti-jamming solutions for 5G and IoT networks. While jamming attacks pose significant threats to the performance and security of these networks, there is a need for a thorough review and analysis of existing anti-jamming solutions, including their strengths, weaknesses, and performance evaluations using experimental simulations and real-world datasets. Additionally, this study aims to identify the key challenges and future research directions in the field of anti-jamming for 5G and IoT networks. By addressing these research objectives, this study seeks to contribute to the advancement of anti-jamming techniques and provide insights for the development of more effective and robust solutions to mitigate jamming attacks in 5G and IoT networks.

JAMMING IN 5G AND IoT NETWORKS

According to (Smith, 2020), 5G and IoT networks are vulnerable to various types of jamming attacks, which can significantly degrade network performance and disrupt critical services.

In this work, the author reviews the different types of jamming attacks that can affect 5G and IoT networks, the techniques used to launch these attacks, and their impact on network performance.

Types of Jamming

Jamming attacks can be classified into two broad categories: intentional and unintentional jamming. Intentional jamming is a deliberate attempt to disrupt wireless communication by transmitting high-power signals in the same frequency band as the legitimate signal. Unintentional jamming, on the other hand, occurs when two or more wireless devices unintentionally transmit signals in the same frequency band, causing interference and signal degradation (Cai et al., 2020).

Intentional jamming attacks can be further classified into three types: continuous wave (CW) jamming, pulse jamming, and random noise jamming (Razaque et al., 2019). CW jamming involves transmitting a high-power signal in a continuous wave, which can effectively block all signals in the targeted frequency band. Pulse jamming, on the other hand, involves transmitting high-power signals in short bursts, which can cause intermittent disruptions to wireless communication. Random noise jamming involves transmitting a high-power signal that contains random noise, which can effectively degrade the quality of the legitimate signal.

Jamming Techniques

Jamming attacks can be launched using a variety of techniques, including direct jamming, reactive jamming, and intelligent jamming. Direct jamming involves transmitting high-power signals in the same frequency band as the legitimate signal, to completely block the signal. Reactive jamming, on the other hand, involves monitoring the wireless channel and transmitting high-power signals only when a legitimate signal is detected. This technique can make it more difficult for anti-jamming systems to detect and mitigate the jamming attack. Intelligent jamming involves using sophisticated algorithms to dynamically adapt the jamming signal to the frequency and modulation characteristics of the legitimate signal (Razaque et al., 2019).

Impact of Jamming on 5G and IoT Networks

Jamming attacks can have a significant impact on the performance of 5G and IoT networks. According to Zhao et al. (2020), jamming attacks can cause packet loss, increased latency, and decreased throughput, which can lead to service disruptions and reduced user satisfaction. Moreover, jamming attacks can be used to launch more sophisticated attacks, such as man-in-the-middle attacks and denial-of-service attacks (Cai et al., 2020).

To mitigate the impact of jamming attacks, various anti-jamming techniques have been proposed, including frequency hopping, spread spectrum techniques, beamforming, and physical layer security. These techniques aim to detect and mitigate jamming attacks in real-time, enabling 5G and IoT networks to maintain their performance and reliability even in the presence of jamming attacks.

In conclusion, jamming attacks pose a serious threat to the performance and reliability of 5G and IoT networks. These attacks can be launched using various techniques and can cause significant disruptions to wireless communication. Therefore, it is essential to develop effective anti-jamming solutions that can detect and mitigate jamming attacks in real-time. The next chapter will discuss some of the anti-jamming techniques that have been proposed to secure 5G and IoT networks.

ANTI-JAMMING TECHNIQUES FOR 5G AND IOT NETWORKS

Frequency Hopping

Frequency hopping is a technique used to combat jamming attacks by dynamically changing the carrier frequency of a wireless signal in a pseudo-random manner. This makes it difficult for the jammer to locate and disrupt the signal. The technique has been used successfully in military communication systems (Cai et al., 2020). In 5G and IoT networks, frequency hopping can be used to improve the resistance of wireless communication to jamming attacks (Razaque et al., 2019).

Spread Spectrum techniques

Spread spectrum techniques involve spreading the signal over a wider bandwidth than required to transmit the information. This makes the signal more resilient to jamming attacks as the jammer would need to occupy a larger frequency band to disrupt the communication. There are two main types of spread spectrum techniques: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) (Zhao et al., 2020).

Beamforming

Beamforming is a technique that involves adjusting the direction of the signal transmission to focus the signal in a specific direction. This technique can be used to improve the signal strength at the receiver while minimizing the signal strength in other directions. This makes the signal more difficult to jam as the jammer would need to be in the direction of the beam to disrupt the communication (Cai et al., 2020).

Multi-Antenna Systems

Multi-antenna systems, such as MIMO (multiple-input and multiple-output) and MU-MIMO (multi-user MIMO), can be used to improve the performance of wireless communication in the presence of jamming attacks. These systems use multiple antennas to transmit and receive signals, which can improve signal quality and reduce the effect of jamming attacks (Razaque et al., 2019).

Physical Layer Security

Physical layer security is a technique that uses the properties of the physical layer of the wireless communication system to provide secure communication. This technique uses measures such as signal encryption and authentication to protect wireless communication from jamming attacks (Zhao et al., 2020), (Aghware et al. 2023), (Yoro et al., 2023), (Malasowe et al., 2023), (Aghware et al., 2024).

In summary, various anti-jamming techniques can be used to secure 5G and IoT networks from jamming attacks. These techniques include frequency hopping, spread spectrum techniques, beamforming, multi-antenna systems, and physical layer security. A combination of these techniques can be used to improve the resilience of wireless communication to jamming attacks.

EXPERIMENTAL EVALUATION OF ANTI-JAMMING TECHNIQUES

Experimental Setup

To evaluate the effectiveness of different anti-jamming techniques, we conducted a series of experiments using a 5G and IoT testbed. The testbed consisted of multiple devices connected through a wireless network, including smartphones, IoT sensors, and a base station. We used a software-defined radio (SDR) platform to simulate jamming attacks on the wireless communication in the testbed. The SDR platform was used to generate jamming signals at various frequencies and power levels as presented in table 1 below.

Table 1: Experimental Setup and Details

Experimental Setup	Details
Testbed	5G and IoT testbed consisting of multiple devices connected through a wireless network
Devices	Smartphones, IoT sensors, and a base station
Software-defined radio (SDR) platform	Used to simulate jamming attacks on the wireless communication in the testbed
Anti-jamming techniques evaluated	Frequency hopping, spread spectrum techniques, beamforming, multi-antenna systems, and physical layer security
Evaluation of techniques	Each technique was evaluated separately, and the experiments were conducted under various jamming scenarios to test their resilience

This study evaluated the following anti-jamming techniques in the experiments: frequency hopping, spread spectrum techniques, beamforming, multi-antenna systems, and physical layer security. Each technique was evaluated separately, and the experiments were conducted under various jamming scenarios to test the resilience of the techniques as represented in table 2 below.

Table 2: Anti-Jamming Technique and Description of Technique

Anti-Jamming Technique	Description of Technique
Frequency hopping	A technique in which the frequency of the transmitted signal is changed rapidly and randomly over a wide range of frequencies
Spread spectrum	A technique in which the signal is spread over a wide range of frequencies, making it more resilient to jamming.
Beamforming	A technique in which the antenna array is used to create a directional beam of radio waves, which can be directed towards the receiver, and thus minimize the effects of interference and jamming.
Multi-antenna systems	A technique that uses multiple antennas to transmit and receive data, increasing the signal strength and resilience to jamming.
Physical layer security	A technique that uses encryption and authentication methods to secure the physical layer of communication, preventing unauthorized access and interference.

RESULTS AND ANALYSIS

The results of the experiments showed that all of the anti-jamming techniques evaluated in the study were effective in mitigating the impact of jamming attacks on wireless communication. Frequency hopping and spread spectrum techniques were effective in improving the resistance of wireless communication to narrowband and broadband jamming attacks, respectively. Beamforming was effective in improving the signal strength at the receiver and minimizing the effect of jamming attacks in a specific direction.

Multi-antenna systems, such as MIMO and MU-MIMO, were effective in improving signal quality and reducing the effect of jamming attacks. Physical layer security techniques, such as signal encryption and authentication, were effective in securing wireless communication from jamming attacks as shown in Table 3.

Table 3: Results and Analysis

Results and Analysis	Details
Anti-jamming techniques evaluated	Frequency hopping, spread spectrum techniques, beamforming, multi-antenna systems, and physical layer security
Effectiveness of evaluated techniques	All anti-jamming techniques evaluated in the study were effective in mitigating the impact of jamming attacks on the wireless communication
Effectiveness of specific techniques	Frequency hopping and spread spectrum techniques were effective in improving the resistance of wireless communication to narrowband and broadband jamming attacks, respectively. Beamforming was effective in improving the signal strength at the receiver and minimizing the effect of jamming attacks in a specific direction.
Effectiveness of multi-antenna systems	Multi-antenna systems, such as MIMO and MU-MIMO, were effective in improving signal quality and reducing the effect of jamming attacks.
Effectiveness of physical layer security techniques	Physical layer security techniques, such as signal encryption and authentication, were effective in securing wireless communication from jamming attacks.
Recommended approach	A combination of these anti-jamming techniques can be used to improve the resilience of wireless communication to jamming attacks in 5G and IoT networks.

Overall, the experiments showed that a combination of these anti-jamming techniques can be used to improve the resilience of wireless communication to jamming attacks in 5G and IoT networks as presented in Table 4.

Table 4: Anti-Jamming Technique and Effectiveness Against Jamming Attacks

Anti-Jamming Technique	Effectiveness Against Jamming Attacks
Frequency Hopping	Effective against narrowband jamming attacks
Spread Spectrum Techniques	Effective against broadband jamming attacks
Beamforming	Effective in improving signal strength and minimizing the effect of jamming attacks in a specific direction
Multi-Antenna Systems (MIMO, MU-MIMO)	Effective in improving signal quality and reducing the effect of jamming attacks
Physical Layer Security Techniques (signal encryption, authentication)	Effective in securing wireless communication from jamming attacks
Combination of Anti-Jamming Techniques	Improves the resilience of wireless communication to jamming attacks in 5G and IoT networks

CONCLUSION

In this study, the researchers explored the problem of jamming attacks in 5G and IoT networks and evaluated different anti-jamming techniques to mitigate their impact. This study identified various types of jamming attacks and their effects on wireless communication. The study also discussed different anti-jamming techniques, including frequency hopping, spread spectrum techniques, beamforming, multi-antenna systems, and physical layer security.

The experimental evaluation of these anti-jamming techniques showed that they are effective in mitigating the impact of jamming attacks on wireless communication. The results indicated that a combination of these techniques can improve the resilience of wireless communication to jamming attacks in 5G and IoT networks.

One limitation of this study is that the experiments were conducted in a controlled environment and may not reflect real-world scenarios. Future work can involve evaluating the anti-jamming techniques in more complex and dynamic environments. Additionally, we only evaluated a limited number of anti-jamming techniques, and there may be other techniques that could be effective in mitigating the impact of jamming attacks.

Another avenue for future work is to explore the potential of machine learning techniques in detecting and mitigating jamming attacks. Machine learning algorithms can be trained to recognize patterns in the jamming signals and take appropriate countermeasures to mitigate their effects.

The findings of this study have practical implications for the design and implementation of 5G and IoT networks. Network operators and designers can use a combination of anti-jamming techniques to improve the resilience of wireless communication to jamming attacks. They can also incorporate machine learning techniques to detect and mitigate jamming attacks in real-time.

In addition, the study highlights the importance of physical layer security in securing wireless communication from jamming attacks. Signal encryption and authentication techniques can be used to secure wireless communication and prevent unauthorized access to the network. Overall, this study provides insights into the problem of jamming attacks in 5G and IoT networks and offers recommendations for addressing this problem. Further research is needed to explore the potential of other anti-jamming techniques and machine-learning algorithms in mitigating the impact of jamming attacks on wireless communication.

REFERENCES

Aghware, F. O., Ojugo, A., Adigwe, A. W., Odiakaose, C. C., Ojei, E. O., Ashioba, N. C., Okpor, M. D., & Geteloma, V. O. (2024). *Enhancing the Random Forest Model via Synthetic Minority Oversampling Technique for Credit-Card Fraud Detection, Journal of Computing Theories and Applications* Vol. 2, No. 2, DOI: 10.62411/jcta.10323 publikasi.dinus.ac.id/index.php/jcta/

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C, Emordi, F. U., & Ojugo A. A., (2023). *DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble, International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 14, No. 6, pp 94-100*, doi:10.14569/IJACSA.2023.0140610

Al-Fuqaha, M., Aledhari, M., Guizani, M., Mohammadi, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials, 17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Malasowe, B. O., Akazue, M. I., Okpako, E. O., Aghware, F. O., Ojugo, A. A., Ojie, D. V., (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 8, 2023.

Cai, W., (2020). A comprehensive survey of wireless security research from the physical layer perspective. *IEEE Communications Surveys and Tutorials, 22*(4), 2355–2394.

Chang, Y., (2020). Experimental evaluation of anti-jamming techniques for wireless communication systems. *IEEE Transactions on Wireless Communications, 19*(3), 1707–1719.

Han, C., Huo, L., Tong, X., Wang, H., & Liu, X. (2020). Spatial anti-jamming scheme for internet of satellites based on the deep reinforcement learning and stackelberg game. *IEEE Transactions on Vehicular Technology*, *69*(5), 5331-5342.

Kim, D. (2019). Experimental evaluation of anti-jamming techniques for 5G wireless communication systems. *IEEE Transactions on Vehicular Technology, 68*(9), 8575–8585.

Li, J. (2020). Experimental evaluation of physical layer security techniques for wireless communication systems. *IEEE Transactions on Information Forensics and Security, 15*, 3611–3626.

Li, M., Li, W., Jiang, W., and Zhu, Y. "A review of anti-jamming techniques in wireless communication networks," in 2017 IEEE 6th International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 81-88.

Lin, K., Yang, H., Zheng, M., Xiao, L., Huang, C., & Niyato, D. (2024). Penalized Reinforcement Learning-Based Energy-Efficient UAV-RIS Assisted Maritime Uplink Communications Against Jamming. *IEEE Transactions on Vehicular Technology*.

Lin, Y. (2021). A deep learning-based anti-jamming algorithm for 5G networks. *IEEE Access: Practical Innovations, Open Solutions, 9*, 21171–21180.

Osseiran, F., Boccardi, F., Braun, V., Kusume, K., Marsch, P., Maternia, M., . . . Fallgren, M. (2014). Scenarios for 5G mobile and wireless communications: The vision of the METIS project. *IEEE Communications Magazine, 52*(5), 26–35. https://doi.org/10.1109/MCOM.2014.6815890

Razaque, A. (2019). Anti-jamming techniques in wireless networks: A survey. *IEEE Communications Surveys and Tutorials, 21*(3), 2066–2101.

Roth, A. E., & Sotomayor, M. A. O. (2020). Two-sided matching: A study in game-theoretic modelling and analysis. Cambridge University Press. https://doi.org/10.1017/CCOL052139015X

Roth, A. E., Sonmez, T., & Unver, U. (2004). Kidney exchange. *The Quarterly Journal of Economics, 119*(2), 457–488. https://doi.org/10.1162/0033553041382157

Smith, J. (2020). Jamming in 5G and IoT Networks: Types of attacks, techniques, and impact on network performance. International Journal of Wireless Networks, 12(3), 45-58.

Sousa, S., Oliveira, D.M.S., Ferreira, R.C., Almeida, A.L.A., and Nascimento, D. "Performance evaluation of anti-jamming techniques for wireless networks," in 2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting, Montreal, QC, Canada, 2020, pp. 1709-1710.

Wu, D., Lei, Y., He, M., Zhang, C., & Ji, L. (2022). [Retracted] Deep Reinforcement Learning-Based Path Control and Optimization for Unmanned Ships. *Wireless Communications and Mobile Computing*, *2022*(1), 7135043.

Yang, H., Xiong, Z., Zhao, J., Niyato, D., Wu, Q., Poor, H. V., & Tornatore, M. (2020). Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach. *IEEE transactions on wireless communications*, *20*(3), 1963-1974.

Yoro, R. E., Aghware, F.O., Malasowe, B. O., Nwankwo, O., Ojugo, A. A., (2023). *Assessing contributor features to phishing susceptibility amongst students of Petroleum Resources Varsity in Nigeria,* Int. J. Elect. & Computer Engr., 13(2), April 2023, pp1922-1931, Doi: 10.11591/ijece.v13i2.pp1922-1931

Yuan, C., Li, M., Zhao, M., & Xu, M. (2021). Physical layer security in wireless networks. *Survey (London, England)*.

Zhang, T., Zhang, Y. J., Li, W. J., Li, J., & Zhang, L. (2017). Beamforming-based anti-jamming in wireless communication systems. *IEEE Communications Magazine, 55*(6), 223–229.

Zhang, Y., et al. (2022). A survey on machine learning for wireless communication security: From theory to applications. *IEEE Journal on Selected Areas in Communications, 40*(1), 146.