A Comparative Study on Anti-Interference Technologies in Modern Communication Satellites

Tianyu Wang

Beijing New Talent Academy, Beijing, China

*Corresponding Author. Email: wangtianyu20@outlook.com

Abstract

In recent decades, the demand for high-quality communication has soared, particularly in the military and healthcare sectors. This study investigates modern anti-interference technologies for communication satellites by synthesizing data from reliable academic resources, including dissertations, journal papers, and periodicals. The research focuses on a comparative analysis of four primary anti-interference methods: frequency hopping, spread spectrum, encryption transmission, and adaptive antennas. Key performance aspects such as signal intensity, anti-interference capability, implementation cost, and complexity are evaluated. The findings indicate that adaptive antenna technology demonstrates superior performance, especially under extreme weather conditions, owing to its unique operational principles and robust anti-interference capabilities. This research concludes that adaptive antennas offer the most promising solution for ensuring stable and reliable satellite communication in challenging environments, and suggests that future advancements will continue to enhance the efficacy of these technologies.

Key words

Anti-interference technology, Communication satellite, Frequency hopping, Spread spectrum, Adaptive antenna

1. Introduction

On May 10, 2024, a G5-level geomagnetic storm struck the Earth, causing significant disruptions to satellite operations. NASA's ICESat-2 satellite lost altitude and entered safe mode, while the Colorado Inner Radiation Belt Experiment CubeSat was prematurely deorbited. The storm's impact extended to ground systems, where GPS-guided tractors deviated from their routes, leading to substantial financial losses for American farmers. In the aviation sector, transatlantic flights were rerouted to avoid communication disruptions and

higher radiation exposure for passengers and crew [1]. The superstorm also disturbed the ionosphere over China, affecting shortwave communication and navigation, damaged an oil pipeline in Australia, and induced high-voltage pulses in submarine cables across the Atlantic and Pacific Oceans. Notably, the United States' GOES-7 satellite lost half of its solar cells, and Japan's CS-3B communication satellite suffered a malfunction in its backup command circuit [2]. These events underscore the critical importance of communication satellites in the modern world and the potential for widespread disaster should they fail.

Communication satellites are fundamental to ensuring signal stability, integrity, system security, and task continuity. They fulfill a variety of crucial functions globally, including internet services, military command and control, meteorological monitoring, and online education, demonstrating their indispensable role in daily life [3]. The primary threat to their operation is interference, which can be malicious, such as from a military electromagnetic attack, or unintentional, arising from extreme weather, interspace phenomena, or equipment malfunctions [4]. Consequently, the implementation of robust anti-interference technology is essential to ensure the normal functioning of communication satellites.

This study aims to provide a comparative analysis of modern anti-interference technologies. The research evaluates four prominent technologies: Frequency Hopping (FH), Spread Spectrum (SS), Encryption Transmission, and Adaptive Antennas. The analysis will firstly detail the principles, advantages, and disadvantages of each technology, along with their most suitable application scenarios. A comprehensive comparison table will then be presented to evaluate these technologies based on four key aspects: signal intensity, anti-interference ability, implementation cost, and complexity. Finally, the study will simulate a specific scenario, such as extreme weather or a military electromagnetic attack, to determine the most effective technology for mitigating interference.

2. Literature review

2.1 Overview of communication satellite systems and interference

A communication satellite system is typically composed of three fundamental segments: the space segment, which is the satellite itself; the ground segment, comprising the terrestrial control and communication stations; and the user segment, which includes the terminals and devices that receive the services [5]. The primary function of these systems is to facilitate long-distance communication. The process begins when a ground station transmits a weak signal to the satellite. The satellite then receives, processes, amplifies, and re-transmits the signal back to a target destination on Earth. Modern systems may employ advanced techniques like dual-beam phased arrays to dynamically track targets and adjust beam direction in real-time, ensuring continuous connectivity [6]. Communication links are established both between satellites (inter-satellite links) and between satellites and ground stations (satellite-ground links), forming complex networks that can span multiple orbital layers (e.g., LEO, MEO, GEO) to optimize for different performance advantages [7] [8].

However, the integrity of these communication links is constantly threatened by various forms of interference. These can be broadly categorized as internal and external. Internal interference includes same-frequency interference, where signals from different beams in a multi-beam system overlap, and beam interference, which occurs between signals of different users within the same beam coverage area [5]. External interference originates from the operational environment, such as other satellites, terrestrial radio sources, or atmospheric conditions. Specific types of interference in satellite constellations include site interference, where two ground terminals are too close to one another, and collinear interference, which happens when a transmitting ground station, a receiving satellite, and an interfering satellite align in a straight line, a significant issue for LEO constellations [9]. Environmental factors, such as climate and the increasing density of Internet of Things (IoT) devices, also contribute to frequency band congestion and signal degradation [10].

2.2 Classification and principles of an-

ti-interference technology

2.2.1 Frequency hopping technology

The fundamental principle of Frequency Hopping (FH) is to rapidly switch the carrier frequency of a signal across a wide band of frequencies in a pseudo-random sequence known to both the transmitter and receiver. By not remaining on any single frequency for a prolonged period, the signal can evade narrowband or partial-band interference. This technique is highly effective for ensuring the reliability of military command communications and can be combined with other technologies to enhance overall satellite resilience [11]. Recent advancements have focused on developing innovative coded FH designs and intelligent, adaptive frequency-hopping patterns to further improve anti-jamming capabilities, especially for direct-to-satellite IoT systems operating in dynamic electromagnetic environments [12] [13].

2.2.2 Spread spectrum technology

Spread Spectrum (SS) technology operates by spreading a narrowband signal over a much wider frequency band. This process reduces the power spectral density of the signal, making it appear as low-level noise to unintended listeners and thus more difficult to detect or jam. An interfering signal at a specific frequency will only affect a small portion of the spread signal's total energy, which can be overcome by the processing gain at the receiver. SS is critical for ensuring the integrity of data instructions sent to satellites and is foundational to high-quality, secure military communications [14]. Modern applications in mega-constellation satellite networks leverage multicarrier spread spectrum (MCSS) to address challenges related to anti-jamming and physical-layer security [15].

2.2.3 Adaptive antenna technology

Adaptive antennas, or smart antennas, utilize arrays of antenna elements and sophisticated signal processing algorithms to spatially filter signals. The core principle involves dynamically adjusting the antenna array's radiation pattern to enhance the reception of the desired signal while simultaneously placing nulls in the direction of interfering signals. This allows the system to effectively "listen" only to the intended signal source and ignore others [16]. This technology is crucial for navigation anti-interference in GNSS applications and for maintaining low error rates in high-speed, dynamic environments by creating signal blind zones to reduce interference [17] [18].

2.2.4 Signal encryption technology

Unlike the previous technologies that focus on avoiding or mitigating the interfering signal itself, signal encryption aims to secure the information content being transmitted. The principle is to encrypt the data using an algorithm, rendering it unintelligible to any unauthorized party that might intercept it. Even if the signal is jammed or captured, the underlying information remains confidential. Advanced techniques in satellite communications now incorporate dynamic or chaotic encryption methods and even quantum-inspired approaches to defend against increasingly sophisticated dynamic risks and cryptanalysis attacks, ensuring a high degree of privacy and security [19].

2.3 Summary and research gap

The existing literature provides extensive analysis of individual anti-interference technologies, detailing their operational principles, advantages, and disadvantages. However, there is a noticeable gap in research that conducts a direct, cross-technological comparison of their performance under specific, challenging conditions. This study aims to address this gap by systematically evaluating frequency hopping, spread spectrum, adaptive antennas, and encryption on a range of metrics, including cost, complexity, and effectiveness. By analyzing their performance in simulated scenarios of extreme weather and malicious attacks, this paper will provide a clearer framework for selecting the optimal anti-interference strategy based on operational context and threat assessment, offering valuable insights for future satellite system design.

3. Methodology

This study employed a secondary research methodology in the form of a systematic literature review. This approach was selected due to the established body of knowledge on satellite communication and the accessibility of extensive online academic databases, which provide a more efficient means of data collection than primary methods such as interviewing research scien-

tists.

The literature search was conducted between June and August 2025 using Google Scholar and other academic databases. The search utilized a range of keywords, including but not limited to: "communication satellite," "anti-interference technology," "frequency hopping," "spread spectrum," "adaptive antenna," "encryption transmission," "satellite interference," and "interference suppression algorithm."

The selection criteria for sources were designed to ensure the currency and authority of the information. The primary inclusion criterion was a publication date after 2019, reflecting the rapid pace of technological advancement in the field. However, foundational papers published prior to this date were included if they established key principles that remain relevant today. Furthermore, sources were vetted for authority, prioritizing peer-reviewed journals and conference proceedings from reputable publishers such as IEEE, Elsevier, Springer, and MDPI. This process ensures the scientific rigor and reliability of the data informing the analysis.

Selected literature was systematically analyzed and synthesized to compare the four chosen anti-interference technologies across four distinct metrics: implementation cost, system complexity, anti-interference capability, and signal intensity. This structured comparison forms the basis for the results and discussion, allowing for a clear evaluation of each technology's relative strengths and weaknesses.

4. Results and discussion

4.1 Comparison of anti-interference technologies

This section provides a comparative analysis of the four selected anti-interference technologies: frequency hopping, spread spectrum, encryption transmission, and adaptive antennas. The evaluation is based on the four metrics established in the methodology: cost, complexity, anti-interference capability, and signal intensity. The findings are summarized in Table 1.

Table 1: Comparative analysis of anti-interference technologies

Technology	Cost	Complexity	Anti-Interference Capability	Signal Intensity
Frequency Hopping (FH)	High ($60,000–$90,000)	High	Strong vs. fixed-frequency; weak vs. wideband jammers	Stable but may fluctuate across channels
Spread Spectrum (SS)	High ($35,000–$60,000)	High	Strong vs. low-power interference; weak vs. high-power jammers	Stable vs. narrowband; degrades under wideband jamming
Encryption Transmission	Moderate (varies)	Low (traditional) to High (quantum)	Secures data only; no direct anti-interference function	Dependent on physical layer; encryption alone does not improve SNR
Adaptive Antenna	Very High ($500,000–$2,000,000)	Very High	Very strong when signal and interference are from different directions	Significantly improves SNR; gain of 6–10 dBi or more

4.1.1 Cost

The implementation cost of Frequency Hopping is high, primarily due to the need for specialized hardware capable of rapid and precise frequency switching, such as high-precision clock chips and frequency synthesizers. The principle of evading interference by constantly changing frequency necessitates that both sender and receiver maintain perfect synchronization, which drives up hardware requirements and cost [13].

Spread Spectrum technology also incurs high costs. Its principle involves dispersing the signal across a wide frequency band using a spreading code, which requires a specialized chip for code generation and a complex

demodulation circuit at the receiver [14]. The hardware must be able to handle a wide bandwidth and complex signal processing, making it significantly more expensive than standard communication equipment.

For Encryption Transmission, the cost varies. While traditional encryption methods can be implemented with relatively low-cost hardware and software, more advanced methods like quantum encryption have extremely high setup costs. However, even standard encryption can reduce overall network investment by leveraging public networks instead of dedicated physical lines, thus lowering expenses related to infrastructure and maintenance [20].

Adaptive Antenna technology is by far the most expensive. Its principle of spatially separating the desired signal from interference requires a large array of antenna elements, each with its own control hardware, and a powerful processing unit to run the complex algorithms that analyze signal direction and adjust the antenna pattern in real-time [16]. The sheer volume of high-performance hardware makes it a very high-cost solution.

4.1.2 Complexity

Frequency Hopping systems are characterized by high complexity. This stems from the intricate hardware and software design needed to ensure perfect, high-speed synchronization between the transmitter and receiver across a constantly changing frequency sequence [11]. Any synchronization error can lead to a complete loss of communication.

Spread Spectrum is also highly complex. The design of the pseudo-random spreading codes is challenging, as they must be sufficiently long and statistically random to be effective. Furthermore, the receiver must be perfectly synchronized with the sender's code to correctly de-spread and reconstruct the original signal. This requires powerful and precise hardware and sophisticated algorithms capable of adapting to a dynamic signal environment [18].

In contrast, traditional Encryption Transmission is relatively low in complexity. It primarily involves software implementation and does not require major hardware modifications or frequent, expensive upgrades. The expertise and personnel required to build and maintain standard encryption systems are also less specialized compared to the other three technologies [20].

Adaptive Antennas represent the pinnacle of complexity. The system must continuously sense the direction and intensity of all incoming signals, distinguish the desired signal from multiple interference sources, and execute complex algorithms to dynamically reconfigure the antenna array's radiation pattern. This constant cycle of sensing, decision-making, and execution in a changing environment requires extremely sophisticated hardware and software integration [17].

4.1.3 Anti-interference capability

The capability of Frequency Hopping is strong against fixed-frequency or narrowband jammers, as the signal simply hops to a different, clear frequency. However, its effectiveness diminishes if the jammer can follow the hopping sequence or if the interference is spread across the entire frequency band [12].

Spread Spectrum is effective against low-power interference because the spreading process lowers the interference's power density relative to the signal. However, it is vulnerable to high-power or wideband jammers that can overwhelm the processing gain of the system. Its effectiveness also fails if the spreading code is compromised [14].

Encryption alone provides no direct anti-interference capability. Its function is to ensure data confidentiality, not signal integrity. The signal can still be jammed or lost. Therefore, it is almost always used in conjunction with other anti-interference technologies like FH or SS to provide a comprehensive security solution [19].

Adaptive Antennas offer very strong anti-interference capabilities, provided the desired signal and the interference originate from different directions. The system can create deep nulls in the direction of jammers, effectively eliminating them. Its primary weakness occurs when the interference is collinear with the desired signal, as the antenna cannot spatially distinguish between them [18].

4.1.4 Signal intensity

In a Frequency Hopping system, signal intensity can be unstable. As the signal hops through different frequency channels, it may encounter varying levels of path loss and fading, causing the received signal strength to fluctuate [11].

Spread Spectrum provides a stable signal intensity when facing narrowband interference. However, strong, wideband interference can degrade the signal-to-noise

ratio even after de-spreading, leading to a weaker effective signal [15].

Encryption has no direct impact on signal intensity. The strength of the received signal is entirely dependent on the underlying physical layer transmission technology. In fact, the overhead associated with encryption can sometimes slightly reduce the effective data rate, but not the signal strength itself [19].

Adaptive Antennas can significantly improve signal intensity. By focusing the antenna's gain in the direction of the desired signal and nullifying interference, the system can dramatically increase the signal-to-noise ratio (SNR). This can result in a signal gain of 6–10 dBi or more, leading to a much stronger and more reliable communication link [17].

4.2 Optimal technology selection for extreme weather conditions

Extreme weather conditions, such as heavy rain or geomagnetic storms, create a highly unpredictable and dynamic interference environment. The interference is unlikely to be confined to a single frequency, and its power can fluctuate dramatically. Furthermore, atmospheric effects can obscure the direction of both the desired signal and the interference sources.

In such a scenario, Frequency Hopping would likely be ineffective, as the interference is not the fixed-frequency type it is designed to counter. Spread Spectrum would also be unreliable; while it can handle low-power, distributed noise, it would be overwhelmed by the high-power bursts of interference characteristic of extreme weather events.

Therefore, the adaptive antenna emerges as the most suitable technology. Despite the challenging conditions, its ability to spatially process signals allows it to locate and track the desired signal while actively nullifying interference from other directions. By dynamically adjusting its directional sensitivity, it can filter out the chaotic environmental noise and maintain a stable communication link. Its inherent capability to increase signal intensity also provides a crucial advantage in overcoming the signal attenuation caused by severe weather [17].

5. Conclusion

This study aimed to identify the most effective anti-interference technology for communication satellites operating under challenging conditions. Through a comparative literature review, four leading technologies, including frequency hopping, spread spectrum, encryption, and adaptive antennas, were evaluated based on cost, complexity, anti-interference capability, and signal intensity. The analysis reveals that while each technology has specific strengths, they also possess distinct limitations.

The results indicate that adaptive antenna technology provides the most robust and versatile solution, particularly for mitigating the unpredictable interference associated with extreme weather. Its unique ability to spatially separate desired signals from noise and dynamically optimize the signal-to-noise ratio makes it superior in complex electromagnetic environments. Although it is the most costly and complex to implement, its superior performance justifies the investment for critical communication systems.

As technology continues to advance, future research will likely focus on hybrid systems that combine the strengths of multiple anti-interference techniques. The integration of artificial intelligence and machine learning into these systems will further enhance their ability to adapt to and counter increasingly sophisticated interference threats, ensuring the continued reliability and security of global satellite communications.

To further this research, future studies of the author should move beyond the theoretical comparison of individual technologies and focus on the development of multi-layered hybrid architectures. For instance, the author should be trying to integrate adaptive antennas with frequency hopping for the mitigation of the inherent weaknesses of each, such as collinear interference and wideband jamming. Furthermore, the incorporation of artificial intelligence and machine learning presents a significant opportunity to transition from static anti-interference patterns to real-time, autonomous threat detection and mitigation. These intelligent systems could analyze complex electromagnetic environments to dynamically select the optimal defense strategy. Additionally, as the industry shifts toward mega-constellations, exploring cost-effective manufacturing for high-complexity hardware will be vital for making adaptive arrays more accessible. Finally, empirical validation through small-satellite prototyping would provide the necessary

experimental data to transition these theoretical frameworks into operational reality, ensuring the next generation of satellite networks remains resilient against both environmental and malicious disruptions.

References

[1] SciTechDaily. (2025). Geomagnetic storm disrupts satellite communications and GPS systems. SciTechDaily. https://scitechdaily.com

[2] Kwak YS, Kim JH, Kim S, Miyashita Y, Yang T, Park SH, Lim EK, Jung J, Kam H, Lee J, Lee H, Yoo JH, Lee H, Kwon RY, Seough J, Nam UW, Lee WK, Hong J, Sohn J, Kwak J, Kwak H, Kim RS, Kim YH, Cho KS, Park J, Lee J, Nguyen HNH, Talha M. Observational Overview of the May 2024 G5-Level Geomagnetic Storm: From Solar Eruptions to Terrestrial Consequences. J. Astron. Space Sci. 2024;41(3):171-194. https://doi.org/10.5140/JASS.2024.41.3.171

[3] Guan, Y. L., & Ge, X. (2022). Satellite communications in the 6G era. IEEE Vehicular Technology Magazine, 17(3), 28–37. https://doi.org/10.1109/MVT.2022.3179359

[4] Geognoss. (2025). Interference sources for communication satellites. Geognoss. https://www.geognoss.com

[5] Zhu, B., Zhen, P., Pan, Z., Zhu, W., Yang, N., & Guo, D. (2026). Joint optimization of multi-beam configuration and resource allocation for low-earth orbit satellites. Physical Communication, 75, 103001. https://doi.org/10.1016/j.phycom.2026.103001

[6] Jiang, H., Qian, M., Wan, C., Chen, Z. N., & Xue, Q. (2025). Wide axial-ratio bandwidth and scanning in dual-beam phased array for SATCOM receiver. IEEE Transactions on Microwave Theory and Techniques, 73(11), 9565–9582. https://doi.org/10.1109/TMTT.2025.3579467

[7] Wang, G., Yang, F., Song, J., & Han, Z. (2024). Free space optical communication for inter-satellite link: Architecture, potentials and trends. IEEE Communications Magazine, 62(3), 110–116. https://doi.org/10.1109/MCOM.002.2300024

[8] Shang, B., Huang, X., Wang, H., Li, X., Tao, M., & Zhang, H. (2026). Multi-satellite cooperative communications for 6G: Fundamentals, system design, and applications. IEEE Communications Surveys & Tutorials, 28, 4690–4730. https://doi.org/10.1109/COMST.2026.3660335

[9] Wang, H., Zou, C., Shao, F., Chang, J., Huang, C., & Li, G. (2025). Collinear interference avoidance strategy for LEO satellite constellation based on transmit beamforming. IEICE Transactions on Communications, E108-B(11), 1324–1337. https://doi.org/10.23919/transcom.2025EBP3043

[10] Chan, C. C., Al-Hourani, A., Choi, J., Gomez, K. M., & Kandeepan, S. (2020). Performance modeling framework for IoT-over-satellite using shared radio spectrum. Remote Sensing, 12(10), 1666. https://doi.org/10.3390/rs12101666

[11] Yu, Z., Hao, Z., Yao, W., & Jia, M. (2023). A capacity enhancement method for frequency-hopping anti-jamming communication systems. Electronics, 12(21), 4457. https://doi.org/10.3390/electronics12214457

[12] Wang, D., Elzanaty, A., & Alouini, M.-S. (2024). Coded frequency hopping for direct-to-satellite IoT systems: Design and analysis. IEEE Internet of Things Journal, 11(22), 36335–36349. https://doi.org/10.1109/JIOT.2024.3404093

[13] Meng, Z., Dai, S., Zhao, Z., Ye, X., Zheng, S., Lou, C., & Yang, X. (2024). Intelligent decision-making for a "three-variable" frequency-hopping pattern based on OC-CDRL. Physical Communication, 66. https://doi.org/10.1016/j.phycom.2024.102434

[14] Zheng, J., Gao, J., Ji, K., & Guo, Y. (2019). Research on anti-interference control technology of satellite communication confidential signal transmission. In 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA) (pp. 226–229). https://doi.org/10.1109/ICSGEA.2019.00041

[15] Yan, W., An, J., Song, J., Li, Y., & Wang, S. (2023). Multicarrier spread spectrum for mega-constellation satellite networks: Challenges, opportunities, and future trends. IEEE Internet of Things Journal, 10(23), 20358–20367. https://doi.org/10.1109/JIOT.2023.3284506

[16] Sun, Y., Xie, J., Gong, Y., Zhang, Z., & Wang, L. (2024). Adaptive interference mitigation space-time array reconfiguration by joint selection of antenna and delay tap. IET Radar, Sonar & Navigation, 18(3), 448–462. https://doi.org/10.1049/rsn2.12489

[17] Tsarik, V. I., & Djigan, V. I. (2025). Adaptive antenna array coupling for anti-jamming GNSS real-time kinematic applications. In 2025 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). https://doi.org/10.1109/SYNCHROINFO65403.2025.11079311

[18] Zhou, W., Zhou, Z., Niu, Y., Zhou, Q., & Ding, H. (2023). A fast anti-jamming algorithm based on imitation learning for WSN. Sensors, 23(22), 9240. https://doi.org/10.3390/s23229240

[19] Kumar, A. K., Quan, C., Houniola, M., Singh, S. S., Kumar, R. R., Assaf, M. H., & Kumar, S. (2025). Advanced encryption techniques in satellite

communications with chaotic injection and quantum collapse for enhanced security. International Journal of Satellite Communications and Networking, 44(2), 158–170. https://doi.org/10.1002/sat.70009

[20] Mahmood, K., Fatima, M. N., Shamshad, S., Ghaffar, Z., Das, A. K., & Alenazi, M. J. F. (2024). A cost-effective key agreement encryption protocol for securing IIoT-enabled WSN communication. IEEE Internet of Things Journal, 12(5), 5185–5193. https://doi.org/10.1109/JIOT.2024.3486044