Analysis Of Deep Learning-Based Anti-Jamming Method for UAV Communication

Shuhan Yang*
School of Automation, Beijing Information Science & Technology University, Beijing, China
* Corresponding Author Email: 13063062833@163.com

Abstract. With the increasing popularity of Unmanned Aerial Vehicle(UAV) in both military and civilian applications, it is crucial to ensure the reliability and safety of their signals. In recent years, deep reinforcement learning has proven to be a powerful tool for meeting this challenge. This paper aims to analyze the potential of deep learning in signal jamming countermeasures for UAV communication systems. Traditional jamming countermeasures, such as frequency hopping and Direct Sequence Spread Spectrum (DSSS), are effective to a certain extent. Still, it is difficult to cope with dynamically changing jamming environments due to single mode and low spectrum utilization. On the other hand, deep learning has powerful automatic feature extraction and pattern recognition capabilities, especially the reinforcement learning method based on deep learning, which can realize real-time adaptation of UAVs to environmental changes and automatic optimization of communication strategies. The article focuses on anti-jamming methods based on reinforcement learning and deep reinforcement learning algorithms and proposes a new anti-jamming strategy for UAV communication based on generative adversarial networks (GANs). Although the deep learning method opens up a new way for anti-jamming of UAV communication signals, it still faces the challenges of high demand for computational resources and complex model training in practical applications.

Keywords: UAVs; anti-jamming; deep reinforcement learning; communication systems.

1. Introduction

With the improvement of UAV manufacturing technology, UAVs have been widely used in many fields, such as agriculture, logistics, military, scientific research, environmental monitoring, and post-disaster rescue, because UAVs can be operated remotely, navigate autonomously and work in extreme environments. Communication systems perform operational commands in these application environments, return feedback information, and transfer data. However, in complex electromagnetic environments, UAVs may face a variety of unintentional or malicious interference in their work. Therefore, to guarantee the safe operation of UAVs, improving their anti-jamming ability is of great significance.

Traditional anti-jamming methods, such as sequence-based frequency hopping and DSSS, have a number of limitations due to their single mode. In frequency hopping, interference immunity is achieved by using a wider frequency range. On the other hand, the spread spectrum optimizes communication signals by expanding them to a larger frequency bandwidth. However, these methods have low spectrum utilization and are usually predetermined in advance. Therefore, they are not well adapted to dynamically changing spectral environments and flexible forms of interference [1].

In recent years, the rapid development of deep learning has provided new ideas for solving the UAV signal anti-interference problem. Deep learning has been applied to the optimization of UAV signals by many scholars thanks to its advantages of strong learning ability, wide-coverage, good adaptability, and good generalization ability. An intelligent optimization method based on reinforcement learning was proposed by Boyang Li et al. [2]. They constructed the perceived interference information as a Markov decision process and optimized it using a reinforcement learning algorithm. Huiting Zhang et al. [3] proposed an anti-jamming strategy for UAV communication by combining time and frequency domains. They utilize dynamic deep double-Q learning structure and energy detection to determine the jamming situation and adopt an intelligent
way to pick the channel and adjust the transmission time. Hence, this kind of method effectively enhances the safety performance of UAV communication.

This paper aims to delve into the value of deep learning in signal jamming countermeasures for UAV communication systems. First, this paper discusses the problem of signal interference in UAV communications while tracing the traditional conventional countermeasures against interference and pointing out their limitations. The basics of deep learning are then introduced and used to elucidate its potential in signal anti-jamming. Subsequently, this paper will explore in detail the deep learning-based signal interference countermeasures in recent years, focusing on the examples of Boyang Li et al. and Huiting Zhang et al. Finally, this paper proposes optimizing UAV signals based on generative adversarial neural networks (GANs), which provides new ideas for future research by scholars in related fields.

2. Signal interference problems

As the key and foundation for the normal and safe operation of UAVs, the UAV communication system is easily interfered or attacked by external signals. The UAV communication system consists of three major parts: the UAV body, the ground station and the information transmission link, each of which has its own unique technical system and operation mechanism. In such complex systems, numerous sensors and communication modules operate in concert in a networked environment and are highly susceptible to diverse security threats. At the same time, the data transmission of drones mainly relies on wireless communication technology, which is susceptible to electromagnetic interference or hijacking and eavesdropping.

A jamming or attack on a drone's communication system can significantly impact the normal operation of the drone and social order. First, certain important data, including some sensitive image and video information may be compromised. Second, the drone's controls may fail, possibly causing it to deviate from its normal course or even force it to land or lose. Last but not least, drones can become unsafe, crash into buildings, be utilized for malicious attacks, or even fly into none-fly zones. Therefore, it is of great practical significance to study the application of communication anti-jamming technology in-depth and extensively in UAV communication systems [4].

UAV communication interference includes natural interference (weather conditions, geography, day/night and seasonal changes, etc.), electromagnetic interference (EMI), human interference (using jammers to send noise signals or beacon signals, etc.), adjacent channel interference, and co-channel interference. In daily life, the more common UAV communication link interference is GPS navigation system interference and telemetry telecontrol signal interference. Telemetry telemetry signal interference may cut off the UAV from the operator and affect the correct reception and feedback of its commands. UAVs rely on telemetry data for environmental sensing and decision-making adjustments. Once telemetry remote control signals are interfered with, they may result in unpredictable flight trajectories or even crashes. In addition, most drones rely on global navigation satellite systems such as GPS to determine their position, speed and time. Suppose the GPS signal is interfered with or blocked. In that case, the drone may deviate from the preset flight route, consume more energy, or even wholly lose its direction in extreme cases, causing damage to the aircraft or other accidents.

There are two main types of telemetry and remote-control signal interference: distributed interference and remote high-power multi-channel interference. Distributed jamming is a form of "face-to-face" jamming, consisting of many spatially distributed jamming units. These units work together to affect and limit equipment such as radars, navigation receivers or communication stations in the larger enemy airspace [5]. There may be many small, lightweight, low-cost electronic jamming devices in the area where drones operate. These devices can be programmed to interfere with selected military electronic equipment automatically. They are randomly distributed and can produce multi-directional interference, causing suppressive interference to UAVs in large areas. Adaptive nulling control may be ineffective if the direction of the interference source exceeds the number of elements
of the adaptive antenna array [6]. Remote high-power multi-channel jamming refers to the ability to jam key nodes of the UAV communication link through spatial power synthesis technology, smart antenna technology and phased array technology. This type of jamming has a wide range of frequency bands and avoids the risk of proximity jamming [6].

In GPS navigation system interference, GPS satellite radio navigation signals are selected for low signal-to-noise spread-spectrum modulation transmission. The time-consuming encoding of GPS military code signals makes it necessary to have high jamming power to counteract the spread-spectrum gain of GPS receivers [6]. Joint radio navigation jamming, including broadcast targeting, broadband blocking and discrete blocking, has the following two main strategies: one is information jamming, which interferes with the correct acquisition and use of navigation information by transmitting high-power noise signals, and the other is destroying the information source, which directly leads to paralysis of the entire navigation system.

3. Traditional UAV communication anti-jamming technology

The problem of signal interference countermeasures has existed for many years. Most of the early jamming countermeasures relied on hardware improvements, such as horn antenna design, directional reception, spectrum hopping, etc. Although these methods are effective, they mainly apply to interference with clear patterns and regularity. Although these methods are effective, they are primarily applicable to interference with clear patterns and regularity. For irregular or dynamically changing interference, they are relatively powerless. In addition, these approaches pose significant challenges to the physical constraints of UAVs (e.g. weight, energy, and cost) as well as the complexity and variability of the UAV communication environment. At the same time, changing environmental factors, including weather changes and building obstructions, can impact the ability of drones to communicate.

With the development of technology, anti-jamming techniques have shifted from early hardware improvements to direct optimization of UAV communication signals. Kalinbacak İ et al. [7] have presented and analyzed in detail the common UAV communication anti-jamming techniques that have been used in recent years for UAV communication. Among them, direct sequence spread spectrum technique and sequence-based frequency hopping are the most widely used in anti-jamming techniques for UAV communication. Extended spectrum technology reduces the power spectral density of UAV communication signals by extending them to a wider bandwidth, thus making the UAV communication link highly anti-jamming and reducing the probability of interception [8]. The DSSS technique is the most widely used extended spectrum technique. DSSS technology expands the spectrum by generating a pseudo-random sequence using a pseudo-random sequence generator, multiplying the pseudo-random sequence with a useful signal, and de-expanding the received signal at the receiving end by transmitting over a wireless channel. DSSS techniques, although easy to implement, have some drawbacks, such as their limited resistance to narrowband and tracked interference [4].

Although these modern approaches mitigate the problem of communication interference to some extent, many challenges remain. First, traditional schemes often require accurate channel state information for optimal anti-interference decisions, but in real wireless environments, accessing this information is difficult. Second, many traditional jamming countermeasures require large amounts of computational resources and energy, which is not feasible for devices with limited size and power, such as UAVs. Finally, the dynamics and complexity of wireless environments and the variability of UAV missions and flight paths require UAVs to be able to respond to and counteract signal interference instantaneously, which is also a challenge. Deep learning methods can learn and extract useful information from incomplete or noisy data and are more robust to inaccurate channel information.

In the future, anti-jamming technologies will be improved at a higher level by introducing artificial intelligence and machine learning technologies so that the drone's communication system can
autonomously learn and adapt to environmental interference. For example, deep learning algorithms can learn from a large amount of UAV communication data to find effective strategies to deal with various types of interference, thus further improving the anti-jamming capability of UAV communication.

4. Deep learning background

4.1. Theoretical foundation of deep learning

Deep Learning is a machine learning subfield, which simulates the human brain's information processing through computational models of neural networks for feature learning and pattern recognition. Neural networks usually contain multiple hidden layers, each with many neurons (nodes). The neural network receives a large amount of input data, which is processed and transformed by neurons and layers to obtain the desired output. The network parameters are trained and optimized through backpropagation algorithms and gradient descent methods to make the network better able to perform specific tasks. In addition, deep learning has shown its powerful ability in many fields, such as image recognition, natural language processing, speech recognition etc.

Deep learning has powerful function approximation and feature representation capabilities. Deep neural networks can automatically find high-dimensional data and represent it in low dimensions. Deep learning can independently learn the features of the complex multi-dimensional environment for the airspace environment, analyze its patterns and discover its characteristics. In the problem of UAV communication against interference, deep learning's powerful pattern recognition ability and automatic feature learning have great potential for application [9].

The use of deep learning makes it possible to perform data-driven interference identification and classification without requiring specific knowledge of the pattern of interference signals. This means that even unknown and complex disturbances can be effectively handled by deep learning. Furthermore, deep learning-based reinforcement learning algorithms provide a way to learn and make decisions in real time in a constantly changing environment. In UAV communication scenarios, reinforcement learning can be used to select the optimal communication method in real time to counteract current signal interference and improve communication reliability.

4.2. Theoretical basis of GANs

GANs, as a kind of deep learning model, are one of the most promising methods for unsupervised learning of complex distributions in recent years. The original purpose of GANs is to generate data that does not exist in the real world, which can be understood as similar to making AIs have creativity or imagination.

The structure of GANs consists of two models: a generator and a discriminator. These two models are trained to play a game-like adversarial game, and the process of GAN training is a confrontation between the generator and the discriminator. The generator processes the random data to make the probability distribution of the data obey a certain distribution and hopes that it is close to the probability distribution of the real data; on the other hand, the discriminator learns the probability distributions of the real data and the generated data and calculates the probability of the input data coming from the real sample distribution, and the result of which is then counteracted in the generator to make the generator produce more realistic data. In the end, the discriminator cannot tell the difference between the generated and real data, and then the Nash equilibrium is reached [10].

5. The application of deep learning in UAV signal interference countermeasures

Reinforcement learning and deep learning methods can effectively help UAVs improve the quality and safety of UAV communication signals when facing electromagnetic interference. In particular, by dynamically adjusting the transmit power and channel selection or by optimizing the decision-
making strategy in the time-frequency domain, the communication reachability of ground users can be ensured while greatly reducing electromagnetic interference, thus improving the communication performance and anti-interference ability of UAVs. This provides stable and efficient communication for UAVs in complex and artificial malicious interference environments.

In order to reduce the UAV's dependence on the electromagnetic environment, Li Boyang et al. [1] optimize the UAV's power adjustment and channel selection by Markov Decision Process (MDP) to improve the UAV's communication performance and anti-jamming ability, and then use reinforcement learning to optimize the UAV intelligently after sensing the jamming information. They proposed a UAV air-to-ground communication anti-jamming method based on the Winning or Fast Learning Policy Hill Climbing Algorithm (WoLF-PHC). The paper's research goal is to maximize the ground users' reachability rate, especially in the face of electromagnetic interference. It is argued that in the face of interference, the UAV's transmit power and channel selection can be dynamically adjusted to circumvent the interference, thus maximizing the reachability of ground users as much as possible.

The paper first constructs a UAV air-ground communication jamming model. A drone tries to send a signal to a ground user, while a malicious jammer generates interference near the ground user, trying to block the normal communication between the drone and the user through electromagnetic interference. Next the basic model of reinforcement learning is constructed. Next, the basic model of reinforcement learning is constructed as shown in Fig. 1. The state represents the discrete information observed from the environment, including the communication channel between the UAV and the ground user in the previous time slot and the interference channel sensed in the last time slot; the action represents the behavior performed by the intelligent body in the current time slot, including the UAV's transmit power and communication channel; the reward function: maximize the reachable rate of the ground user while taking into account the power consumption of the UAV and taking into account the relevant parameters of the transmit power and the channel. Parameters are taken into account.

The article also presents the electromagnetic interference sensing based on Long Short-Term Memory (LSTM) neural networks method [11] for obtaining information about the adversary channel. Once the UAV acquires the last interference information through electromagnetic interference sensing, it optimizes its anti-interference decision based on the communication quality information from the link. Then, the decision-making process is trained by the reinforcement learning algorithm, which ultimately increases the user reachable rate and reduces the signal-to-noise ratio.

Huiting Zhang et al. [2] proposed an anti-jamming strategy for UAV communication that combines time and frequency domains. They employ a dynamic deep double Q learning (D-DDQN) architecture to detect interference situation through energy detection and optimize the greedy strategy to cope with the environmental changes. In addition, they treat the decision-making process as a sequential problem to intelligently select channels and adjust transmission times, effectively enhancing UAV communications' security. The input of the model is the interference discrimination style information, while the output of the empirical pool is the optimal policy estimate $\pi$ and the utility value function.
6. Uav communication anti-jamming based on GANs

This paper proposes a GAN application for UAV anti-jamming based on the above research. The input signals for GAN model training are the uninterfered UAV signal samples (labeled as non-interfering signals), and the interfered UAV signal samples (labeled as interfering signals). As shown in Fig. 2, in the GANs network model, the task of the generator is to produce a synthesized signal that is as close as possible to the actual interference-free signal. The discriminator’s task is to classify whether the signal it receives is a valid interference-free signal or a synthetic signal generated by the generator.

Fig. 2 GANs training model

The output of the trained GAN model is an anti-interference signal generated by the GAN, which should be as close as possible to the real interference-free signal and can cancel out the interference components in the actual received signal. Therefore, in UAV communication, as shown in Fig. 3, each time a signal is received, a "pseudo" interference-free signal is simultaneously generated using the trained generator. This signal cancels out the interference in the actual received signal, and a relatively "pure" signal is obtained. This "pure" signal is then used to make the next action or decision as if it had been received without interference.

Fig. 3 Anti-jamming Implementation Ideas

In addition, GAN can also simulate real jamming signals and complex placement environments to generate more realistic and complex jamming samples. This increases the training data's richness and the model's flexibility. When learning and training with reinforcement learning models such as DQN or traditional Q-learning, the interference samples generated based on GAN can be used as a more realistic training environment, so that the UAV communication anti-jamming system can learn and adapt to more interference scenarios in the simulated environment and enhance the anti-jamming capability.

7. Conclusion

This study analyzes that deep learning has a relatively large potential in the UAV communication signal jamming filed. Although traditional anti-jamming schemes such as frequency hopping and spread spectrum can solve the communication jamming problem to a certain extent, they are difficult to cope with the dynamic spectrum environment. The advantages of deep learning are as follows: first, deep learning has the ability of automatic feature extraction, so it can deal with complex airspace environment and information interference; second, deep learning has excellent pattern recognition ability, and it can effectively recognize and classify unknown and complex interference patterns. Third, using the reinforcement learning algorithm based on deep learning, the UAV can learn and adapt to the environment in real time. Thirdly, the deep reinforcement learning algorithm is used to
select the optimal communication strategy to resist the current signal interference in real time to improve communication reliability.

This thesis focuses on the third advantage, and briefly introduces two examples of deep reinforcement learning on UAV communication anti-jamming. One is the use of the WoLF-PHC learning strategy of reinforcement learning to train and learn from UAVs to enhance their anti-jamming capability; the other is the use of energy detection to determine the jamming situation and the use of D-DDQN to select the channel and adjust the transmission time rationally. Both examples demonstrate once again the capability of deep learning in communication jamming. Finally, I will propose a new method based on GANs to optimize UAV communication to enhance its security.

This paper aims to discuss and illustrate the potential of deep learning in signal jamming countermeasures for UAV communication systems. The advantages of deep learning are illustrated by listing some traditional countermeasure techniques and modern deep learning solutions for UAV communication jamming. It also proposes a strategy for GANs to be applied to UAV communication anti-jamming, which provides new ideas for future research in related fields.

References