Al-Qadisiyah JournalFor Engineering Sciences xx (20xx) 001 – 010

Contents lists available at: http://qu.edu.iq

Al-Qadisiyah Journal for Engineering Sciences

Journal homepage: https://qjes.qu.edu.iq

Review paper

A comprehensive survey on jamming and anti-jamming techniques in radar systems

Tabarek M. Makki [1], ***Ghufran M. Hatem*** [1]**, and *Maytham K. Abbas*** [2]

[1]*Department of Communication Technical Engineering, Technical Engineering College, Najaf, Al-Furat Al-Awsat Technical University (ATU), Iraq.*
[2]*National University of Science and Technology, 119049, Moscow, Leninsky Prospekt, 4, building 1, Russia.*

ARTICLE INFO

Article history:
Received 00 mmm yyyy
Received in revised form 00 mmmmm YYYY
Accepted 00 mmmm yyyy

keyword:
Radar
Radar techniques
Radar countermeasures
Radar jamming
Rradar anti-jamming

ABSTRACT

This article presents a survey on radar jamming and anti-jamming techniques. With the improvement of modern warfare technologies, electronic warfare faces increasingly challenging occurrences. Radar plays a crucial role in electronic warfare and is utilized in various applications such as air traffic control, aircraft anti-collision systems, and radar antimissile systems. However, radar systems are susceptible to electronic countermeasures, particularly jamming devices. Jammers emit jam signals to disrupt and deceive radar systems. This article explores the concept of radar jamming, including its working principles and techniques. It also highlights the importance of anti-jamming technologies to protect radar systems. The importance of understanding the environment and the capabilities of jammers has been emphasized to develop secure and effective anti-jamming systems. The study emphasizes the interplay between jamming and anti-jamming techniques, with advancements in one driving the development of the other. The paper concludes by providing an overview of the discussed topics and their significance in the field of radar technology.

1. Introduction

With the development of modern warfare technologies, electronic warfare encounters a more difficult circumference. Radar is the essential weapon of electronic war, which has been used in air traffic control, aircraft anti-collision systems, flight control systems, radar anti-missile systems, and other applications. Because the working of radar is more important and in wide ranges, the enemy would be highly motivated to take advantage of the information, also the environment that radar working on it could affected by many electronic countermeasures like jammers [1]. Jammers a device that are used to generate and emit a jam signal to the intended device (radar), which works to deceive and disrupt the radar [2]. The process of sending energy to the victim device in a specific time and place is defined as Jamming, the working principle of any jammer device is to overwhelm the power that has been transmitted to the threat device [3]. This process is done by amplifying the jamming signal before sending it to the victim device [4]. Therefore, Jamming can be defined as the process of preventing the receiver (Rx), in a transversing system, from understanding the meaning of the information included in the received signal. Jammers work either by a given RF signal or by generating a signal of equal frequency with the required device to be jammed. Also, the power, used by the jammer, must be much higher than the power in the targeted device and the targeted device will receive the higher power of the jamming random signal, which is more effective than the information signal. Consequently, it will not be able to operate correctly [5, 6]. There are limitation factors to any jammer device which are: the transmitted bandwidth, and the transmitted power which means that you should have many types of jamming signals and apply them to different applications [1]. However, the jamming signal may be expressed by random noise, and keep in mind that jammers can operate with single or multiple frequencies [5, 6]. With the decreasing demand for the applications of radio signals, there are many developments in consumer devices. Radio signals have many applications such as Mobile broadband and telephony, WIFI and Bluetooth connections, and Radar [7]. But, by using signal jamming devices, these services could be blocked either intentionally using jammer devices or simply by interfering with the other transmission process [7]. Figure 1 illustrates the common types of radio frequency jammer signals. So, anti-jamming (countermeasure) technologies are necessary and required to protect the radar, to have a secure and effective anti-jamming system, it's important to know the environment and jammers if we don't have this information can't depend upon the radar decisions. Radar is an acronym for Radio Detection and Ranging which is defined as a device used for detecting specific parameters of any object when the radar transmits RF signal then receives and detects the reflected signal from the target devices. The reflected signal is then analyzed and processed to find the required data such as distance, velocity, angular position, etc. [8–10]. Many criteria may be used such as resolution which works to determine how much the ability of a radar to discover various targets[11]. With the development of radar devices in the wars the equipment of anti-radar has been developed rapidly to decrease their performance. The jamming and anti-jamming are completely two obverse techniques, the discovery of a new jamming technology will lead to discovering a new anti-jamming technology, also new interference will necessarily lead to new radar anti-jamming techniques. So this cycle results to find a development in the jamming and anti-jamming techniques in radar devices [12, 13]. This survey covers a wide range of topics, including jamming waveform design, anti-jamming signal processing algorithms, and emerging technologies.

*Corresponding Author.
E-mail address: tabarak.ms.etcn46@student.atu.edu.iq ; Tel: (+964) 780-716 8403 (Tabarek Makki)

https://doi.org/10.30772/qjes.000.000.000

Nomenclature

B	Communications receiver bandwidth	P_j	Jammer power
J/S	Jamming to signal ratio	G_{jr}	Antenna gain from the jammer to the receiver
P_t	Transmitter power	G_{tr}	Antenna gain from transmitter to receiver
G_{rj}	Antenna gain from receiver to Jammer	B_j	Jamming transmitter bandwidth
G_{rt}	Antenna gain from receiver to transmitter	R_{jt}	Range between jammer and communications receiver
R_{tr}	Range between communications transmitter and receiver	L_r	Communication signal loss
L_j	Jammer signal loss (including polarization mismatch)		

Furthermore, the survey explores the effectiveness and limitations of existing solutions, highlighting areas for future research and development. By consolidating the current state-of-the-art jamming and anti-jamming radar techniques, this paper aims to provide a valuable resource for researchers, practitioners, and system designers involved in the field of radar technology, enabling them to enhance the resilience and reliability of radar systems in the face of intentional interference. [1].

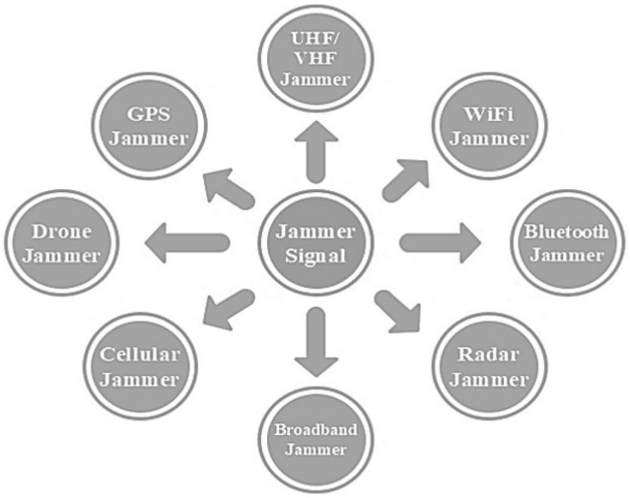

Figure 1. Common Types of Radio Frequency Jammer Signals.

2. Jamming to signal ratio (J/S)

Jamming to signal ratio is the measure of jamming signal strength (J) to the strength of echo signal (s), which is termed J/S and its measure unit in dB [14]. The effectiveness of a jamming device depends upon several parameters which are:
- Jamming to Signal ratio
- Channel coding, and
- Type of modulation techniques [15].

However, jamming to signal ratio equation expressed as in Eq. 1.

$$\frac{J}{S} = \frac{P_J\, G_{JR}\, G_{RJ}\, R_{TR}^2\, L_R\, B_R}{P_T\, G_{TR}\, G_{RT}\, R_{JR}^2\, L_J B_J} \tag{1}$$

where;
P_j =Jammer power
P_t = Transmitter power
G_{jr}= Antenna gain from the jammer to the receiver
G_{rj}= Antenna gain from receiver to Jammer
G_{tr}= Antenna gain from transmitter to receiver
G_{rt}= Antenna gain from receiver to transmitter
B_r = Communications receiver bandwidth
B_j = Jamming transmitter bandwidth
R_{tr}= Range between communications transmitter and receiver
R_{jt} = Range between jammer and communications receiver
L_j = Jammer signal loss (including polarization mismatch)
L_r = Communication signal loss [14–18]

3. Radar jamming techniques

The main purpose of the jammers is to fill the radar receiver end with a noise signal to disrupt its working where the main task for any receiver system is to extract the required parameters from the received signal[20]. Radar jamming works by blocking, interfering, and decaying the radar system, so the radar can't detect and find targets exactly [19]. However, there are several types of radar jamming, categorized into three sections are shows in the Fig. 2 below and all will be illustrated in details below:

3.1 Section 1

Depending upon the type of signal to be used in the transmitting system there are two types of jamming, mechanical and electrical jamming. They are briefly illustrated below:

3.1.1 Mechanical jamming

This mechanism is caused by different devices that reflect the transmitted energy to the transmitter. This produces what's named, in radar systems, as the false target which returns to the operator's scope. Mechanical devices are divided into three major types; chaff, corner reflectors, and decoys [6].

- Chaff a radar attack utilizing small, thin pieces of aluminium, metalized fiberglass, or plastic to create a cloud, making it seem like a cluster of primary targets or producing numerous returns on the radar screen [20].
- Radar decoys The goal of a decoy is to deceive sensors into thinking it's the real thing and draw their attention. Active decoys work by receiving radar signals, amplifying them, and retransmitting them in real time, resulting in a significantly larger radar cross-section (RCS) [20].

3.1.2 Electrical jamming

In electronic jamming, highly power-interfering signals are radiated toward the radar (targeted device) which leads to blocking the process of receiving. Electronic jamming is divided into two major styles; Noise and Repeat techniques. The noise technique is further divided into three types; spot, sweep, and barrage [6]. All will be illustrated below:

- Noise jamming this is a continuous random signal used to hide the echo signal from the enemy radar [20]. Simplicity is the main advantage of noise jamming also detailed information for the used radar signal is not required. For effective noise jamming, the energy of noise jamming should be more than the echo signal [4]. One of the most important disadvantages of noise jamming is the radar employer can understand that the radar has been jammed by a noise jamming source from the radar display screen [2]. There are several types of noise jamming and some of them are introduced below:

- Jam on Tune: this is the first and simplest type of jamming, used in enemy transmission to detect a target in specific frequency and bandwidth. As illustrated in Fig. 3 it works by tuning the jammer device to the specific frequency and bandwidth then turning it on, after a specific shorty time will be turned off to survey if the target still exists [1].
- Barrage Jamming: working by transmitting noisy signals across a wide range of frequencies to the radar signal. Barrage jammers can jam different ranges of frequencies and different radars because of their working capability with wide bandwidth, it's also called multi-channel jammers and multi-tone jammers [2]. The main disadvantage is only part of the jam signal will be received because of its transmission to a wide range of spectrum. Therefore, a high jamming noise signal must be sent to control or disrupt the reflected echo signal [3, 4, 20]. Thus, the advantages of a barrage jammer simply lie in its capability to transmit over broads of bandwidth, the other advantage may convert into a disadvantage point when the radar system works with highly transmitted power, the jammer will not be affected by the echo signal because the jammer power will not be adequate to interfere with the reflected echo signal sufficiently [2]. When increasing the number of the required jammed frequencies, will lead to more power to sufficiently decrease the SINR (signal-to-interference noise ratio) [2]. Figure 4 shows the spectrum signal of barrage jammer.
- Base jamming: is a form of barrage jamming working by jamming only one radar device at all frequency ranges [20].

- Spot Jamming: also called single-channel jammer and a single-tone jammer, working by targeting spot frequency (single frequency)[2], that's done by transmitting all jamming energy to a narrow spectrum, but to ensure that the jammer device is effectively jammed the reflected echo signal requires info about the system operation frequency if this is available to the jammer device means the radar will be jammed successfully. If the operation frequency is not known by the jammer, jamming the radar with spot jamming may be impossible. To jam different radar devices with spot jamming, multiple jammer devices will be required [4, 20]. Spot jamming prevents the radar from measuring the required parameters for the target such as range, angle, and type of modulated signal that is used in the receiver [21]. The main advantage of spot jamming is all the jamming power is cantered in a specific portion of the spectrum, so it can disrupt the radar or any communication device for a longer distance [21]. Figure 5 illustrates a simple comparison of the frequency range between barrage and spot jamming signals.
- A jammer device that emits all of its noise power to the bandwidth of the radar receiver is called a spot jammer, while the jammer that radiates all of its power into a broad of frequencies is called a barrage jammer. Sweep Spot jammer is a combination of these jammers [21]. Also called scan jammer and follow-on jammer [2]. Barrage jammer emits a broad of frequencies so it will jam the radar definitely, but a lot of the jamming power will be lost. Otherwise, spot jamming could be an effective jammer if the frequency of the jammer matched with the radar operation frequency. Thus, sweep spot jammers are found to solve this problem that has transmitting a narrow band jamming signal with a swept frequency across the wide spectrum so that different radars will be jammed as shown in Fig. 6 [4, 20]. It's divided into:
  - Sequential jammers that scavenge the spectrum signal from higher to lower frequencies or from lower to higher [2].
  - Non-sequential jammers which don't follow a constant sweeping model [22].

  A swept jammer could be used when the target changes its frequency rapidly or if there are multiple signals to be jammed [3]. Swept jammers have the advantages of emitting noise power in a narrow band (spot jammers) and the effectiveness of covering a broad bandwidth [21]. The most important disadvantage is that by using modern radar systems sweep jammers could be easily detected and then avoided by adapting the operation frequency of the system [21]. Sweep jammer can be easily anti-jammed by using an efficient learning-based anti-jamming technology [23].
- Adaptive jammer: this type of jammer is used when required to jam several frequencies. Figure 7 illustrates the working principle of the adaptive jammer, which operates by dividing the available power into several necessary. When required to add a new channel the power that is required to each channel will reduce, because the total power of the jammer device is restricted. For example, if we have two channels to jam the total power of the jammer device will divided into 2 to get each channel with equal powers [2, 3, 24].
- Random-selection jammer: as obvious from its name random selection jammer works on selecting frequency from a set of frequencies to be jammed so that the process of selecting a frequency band doesn't depend upon the prior band [2, 25].
- Static jammer: this jammer is the easiest model that jams simultaneously specific channels at the same time and frequency, and simply could be cancelled by changing the channel that was jammed [26, 27].
- Constant jammer: A constant jammer randomly generates and emits continuous RF (radio frequency) signal but in this case will have a large disadvantage which won't be energy efficient [2].
- Random jammer: works by randomly transmitting a jamming signal to the target network and randomly selecting the desired time slot to jam, then sleeping in the rest duration [2]. This alternative method between jam and sleep periods makes the jammer more energy efficient than the constant jammer [2]. This jamming technique is highly effective, but unfortunately could be detected easily [24].
- Pulse jammer: this jammer uses pre-decided jamming and sleeping durations and many times these periods are almost equal [2].
- Repeater Techniques: In this technique, the approach of Digital Radio Frequency Memory (DRFM) is applied. The transmitted targeted frequency is captured by the DRFM. Thereby, the value of jamming frequency is determined and repeated to the communication channel of the targeted system. This is why this technique is called Repeater jamming. In radar applications, the range of the radar detection could be changed which could apply when the received radar energy is manipulated and retransmitted to change the return of the radar sees. [6] DRFM jammers could be easily detected by the radar system because of it transmit the jam signal beyond to the returned signal (echo signal). So that several types of repeater jammers are proposed to overall the drawbacks of DRFM jammers. Such as frequency-shifting jammer interrupted sampling repeater jammer (ISRJ), and the spectrum-dividing jammer [28, 29]. Figure 8 presents a brief schematic overview of radar jamming techniques that rely on signal transmission.

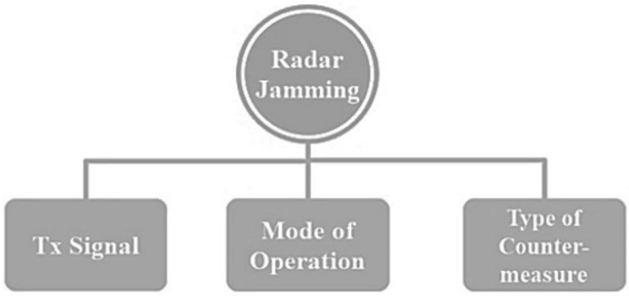

Figure 2. Schematic of the main categories of radar jamming techniques.

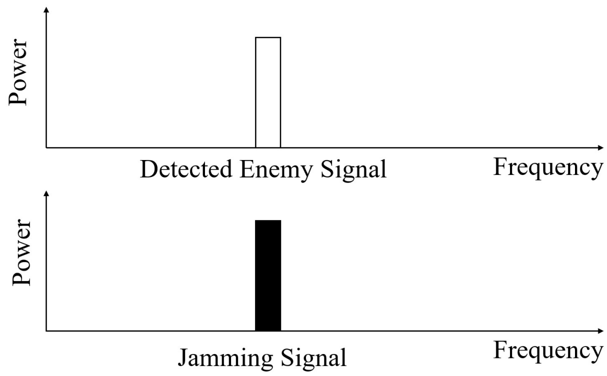

Figure 3. Spectrum of Jam On Tune jammer [3].

Figure 4. Spectrum of Barrage Jammer [3].

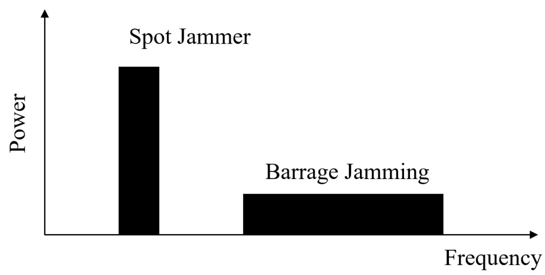

Figure 5. Difference between Barrage and spot jammers in freq.ranges [2].

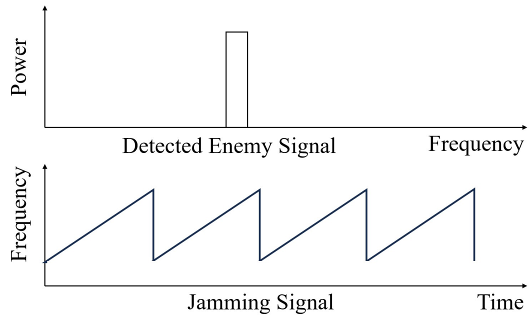

Figure 6. Spectrum of Sweep Jammer [3].

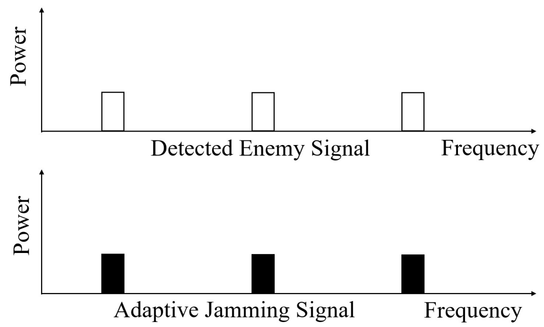

Figure 7. Spectrum of Adaptive Jammer [3].

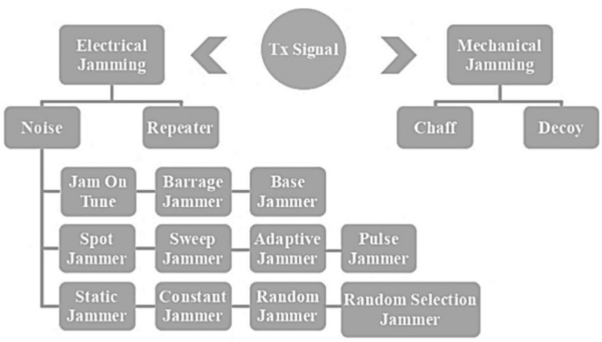

Figure 8. Schematic describes radar jamming techniques based on transmitting signals.

3.2 Section 2

based on the mode of operation radar jamming divided into two types are suppressing jamming and deception jamming:

3.2.1 Suppressing jamming

or cover jamming used to cover a range of frequencies, is used to decrease the ability of enemy radar to detect targets or work to detect false targets, suppressing jamming is divided into two types which are active suppressing jamming and passive suppressing jamming. Passive suppressing jamming affects target detection while active suppressing jamming works on generation jamming signals with high power thus jamming signal will be received by radar and affect the process of target measurement. Active suppressing jamming contains both noises suppressing jamming and dense false target jamming. Noise suppressing jamming works to decrease the SNR of the radar system therefore decreasing the ability of the operation of a radar system to detect and measure the process of the target. While dense false jamming works by producing several targets the radar will detect many targets and cannot distinguish the real one [19]. Suppressing jamming can be employed to deceive the radar by creating fictitious targets or by replicating an actual target's features, and could be avoided using an advanced radar system that uses modern strategies like frequency hopping or spread spectrum [30].

3.2.2 Deception jamming

working by generating a signal that is similar to the returned echo signal by fully the radar receiver with false target information this is done by emitting, transmitting, or reflecting EM waves. According to the echo signal that carries false information deception jamming will be divided into [19]:

- Range deception: or called by range gate pull-off technique,
- Velocity deception: called by the velocity gate pull-off technique, and
- Angle deception: sometimes for conical scan radar, called inverse gain jamming, and for single pulse radar, called eye jamming or cross-polarization jamming [?, 19].

By using modern radar systems, deception jammers could be easily detected and then avoided by adapting the operation frequency of the system [31]. Figure 9 below describes a brief schematic summary of the above-illustrated radar jammer technologies based on the effect. All these types work by making the radar generate false velocity, angle, and range info about the target according to the received false echo signal [19].

3.3 Section 3

Radar jamming is divided into two types based on the signal generation method (type of countermeasure) of active jamming and passive jamming:

3.3.1 Active Jamming

used to jam a range of frequencies. It works by transmitting an electromagnetic wave (EM) to decrease the capability of enemy radar to detect and track the target. Classic active jamming involves noise jamming, repeater jammer, and more [19]. Active jamming's major disadvantage is that it can provide the enemy radar system access to the jammer's position [19]. It produces a jamming signal that is adjusted to match the frequency and modulation of the radar signal, therefore making it impossible for the radar to distinguish between the two signals [32].

3.3.2 Passive Jamming

instead of generating their electromagnetic waves, passive jamming devices reflect or absorb them to disrupt and diminish enemy radar detection and tracking. Common examples of passive jammers include angle reflectors, passive decoys, chaff, and more [19].

- Table 1 illustrates a simple comparison between the most commonly used jamming techniques.
- All these types work by making the radar generate false velocity, angle, and range info to the target according to the received false echo signal [19].

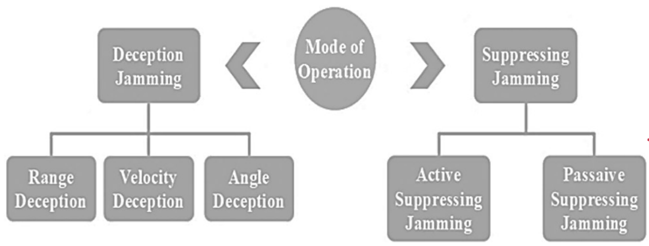

Figure 9. Schematic of radar jamming techniques based on the mode of operation.

4. Radar anti-jamming techniques

In the challenges between radar and jammer devices, jammers are working on improving the jamming technologies to produce a novel and more complex jammer model [33, 34]. In this section, we will introduce many types of Radar anti-jamming technology, which is a part of radar technology and can't be completely separated [19]. Because of the increasing challenges between radar jamming and anti-jamming techniques, the researchers focused more on the development of anti-jamming technologies [35]. Radar anti-jamming technologies are used to test if the electromagnetic spectrum is used effectively to deal with electronic interference [36, 37]. Radar anti-jamming is an electronic warfare in the electronics domain, where any radar could be jammed, and any jamming signal (source) could be blocked. The major idea for the anti-jamming process is to keep the radar working in normal conditions by decreasing the external interfering signals that work to affect the radar operation, and also keep them at an acceptable level [37]. Radar anti-jamming techniques are divided into two methods, which are:

Table 1. A Simple comparison between the commonly used jamming signals.

Jamming type	Bandwidth	Advantages	Disadvantages
Noise	Transmits a continuous random signal in the frequency domain [20].	Not required detailed information for the used radar signal [4].	Using the radar's display screen, the radar employer could understand that the radar has been jammed [2].
Barrage	Transmits jam signal over a wide range of frequencies [2].	Because of its capability to transmit over a broad bandwidth, barrage jamming can jam different ranges of frequencies and different radars [2].	A high jam noise signal must be sent to disrupt the reflected echo signal because only part of the jam signal will be received due to its transmission over a wide range of spectrum [3, 4, 20].
Spot	Transmits jam signal over a narrow spectrum [4, 20].	It can disrupt the radar or any communication device over a longer distance because all the jamming power is centred in a specific portion of the spectrum [21].	Needs to acknowledge the radar's operation frequency, without this info, jamming the radar using a spot jammer could be impossible [?, 4].
Sweep	Transmits narrow band jam signal with a swept frequency across a wide spectrum [?,4].	Emits noise power in a narrow band, and have the effectiveness of covering a broad bandwidth [21].	Using modern radar systems, sweep jammers could be easily detected and then avoided by adapting the operation frequency of the system [21]. Could be easily anti-jammed by using an efficient learning-based anti-jamming technology [23].
Adaptive	Transmits jamming signals over several frequencies [?, 2].	Jam multiple radars simultaneously [3].	The total power of the jammer device is restricted because when required to add a new channel to be jammed the power that is necessary for each channel will decrease [2].
Suppre	Transmits signals over a wide bandwidth [19].	Used to deceive the radar by creating fictitious targets or by replicating an actual target's features [30].	Simply could be avoided using advanced radar systems that use modern strategies like frequency hopping or spread spectrum [30].
Deception	The range of frequencies that have been used is not specified, it varies depending on the specific jamming system and the type of radar being targeted [38].	Generate a signal that is similar to the returned echo signal by full the radar receiver with false target information this is done by emitting, transmitting, or reflecting EM waves [19].	Using modern radar systems deception jammers could be easily detected and then avoided by adapting the operation frequency of the system [31].
Active	Transmits jam signal over a range of frequencies [19].	produce a jamming signal that is adjusted to match the frequency and modulation of the radar signal, therefore making it impossible for the radar to distinguish between the two signals [32].	The major disadvantage is that it can provide the enemy radar system access to the jammer's position [19].

- Technical anti-jamming method: also distinguished into two categories: blocking the jamming signal from entering the receiver by objection it outside the receiver, and if the jamming signal successes in entering the receiver, it is important to utilize the different attributes of both the jamming signal and the target signal from the jamming signal,
- Tactical anti-jamming method, The essential radar system components are shown in Fig. 10 below which are the radar antenna, radar signal processing system, radar transmitter and receiver system, etc., these are the carriers of anti-jamming measures and all will explained in detail below [1, 39].

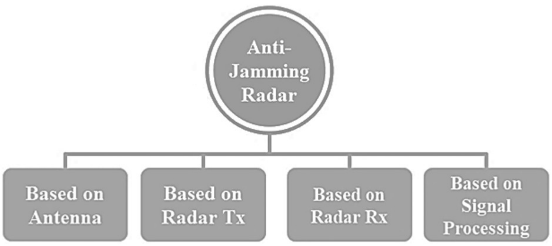

Figure 10. Schematic diagram of the essential radar anti-jamming techniques.

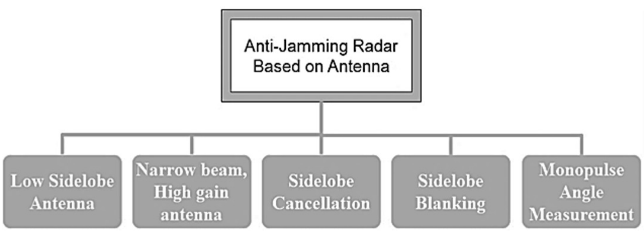

Figure 11. Types of radar anti-jamming techniques based on antenna.

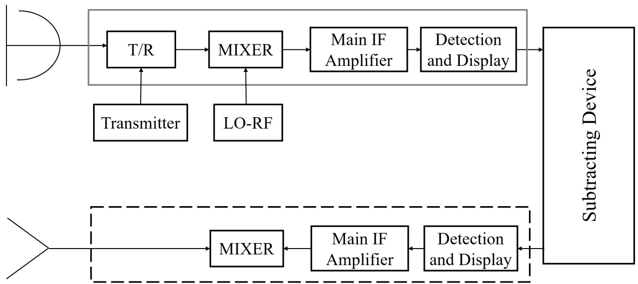

Figure 12. Schematic diagram of sidelobe cancellation system [34].

4.1 Radar Anti-jamming Technology Based on Antenna

Based on radar antenna, anti-jamming technologies are divided into many kinds as shown in Fig. 111 below and all will explained in detail such as low sidelobe antenna, narrow-beam high gain antenna, sidelobe blanking, sidelobe cancellation, and monopoles angle measurement [1, 39].

4.1.1 Low sidelobe antenna

Low sidelobe antenna affects the sidelobe interference while sidelobe jamming works to affect the sidelobe of radar transmitting signal [39], because the radar antenna's main lobe has properties of narrow with a high gain and highly strong directivity, while the sidelobe of radar antenna is broad, so the interference signal typically enters the receiver's antenna from the sidelobe. Because the jammer and target signals are too close to each other and both of them are in the main beam lobe main lobe jamming is one of the most difficult jamming types [1, 40]. Low sidelobe antenna consists of:

- low sidelobe transmitting antenna used when transmitting signals to minimize the probability of interfering with jam signal and reduce the eventuality of jamming signals to enter the system through sidelobe [19], and

- low sidelobe receiving antenna [37]. A new method of sidelobe has approached using beam pattern and adaptive digital beam forming, which is used to reduce the jamming effects but this method won't work if the jamming plan on the sidelobe is too high [1, 41].

Another method of pulse compression is achieved to conflict the sidelobe jamming its main purpose is to accomplish a required level of SNR this process is done by transmitting a signal with a long length, this method works by combining both short pulse resolution and long pulse energy signifying [1]. However, there are also snags when using the pulse compression method because its transmitter and receiver are complex and include time-side lobes [1].

4.1.2 Narrow beam, high gain antenna

The interference radiation area and the interference ratio could be effectively controlled using the characteristics of narrow beam and high gain antennas. Also, the narrow beam antenna has the characteristic of high energy density and is fixed in a specific direction [39]. Therefore, these characteristics achieved many advantages such as:

- Reduce the multi-path effects by reducing the ground reflection and increasing the radar countermeasure distance,
- SINR of the received signal is controlled, and
- Decrease the district of the jamming beam of the jammer to be equal to the received signal beam of radar [39].

4.1.3 Sidelobe cancellation

The Sidelobe cancelation method has two operating methods:

- Open loop: the major advantage is that has a very short convergence time, and
- Closed loop: has a too-long convergence time which forms a major disadvantage [19].

To design a typical low sidelobe antenna model, sidelobe cancellation techniques almost used, the use of sidelobe cancellation techniques working on blocking the interference coming from the sidelobe without affecting the effectiveness of the antenna's main lobe [39]. Figure 12 below shows the schematic diagram of the sidelobe cancellation system, which consists of two receiving channels that are connected respectively used to receive the radar echo signal one of these is named the main receiving channel and the other is the auxiliary receiving channel [39]. The gains of both receiving and auxiliary channels that are used in the transmission are balanced, the jamming signal that enters from both sidelobe and auxiliary antennas could be canceled using the subtractor, then the jamming signal that entered by sidelobe antenna will be restrained, and the effectiveness radar's main lobe antenna will not be affected [39]. Performance analysis of an open loop sidelobe cancellation has been discussed using a variable of cancellation ratio concerning

- Phase center of the auxiliary antenna,
- Jammer's direction of arrival, and
- Jammer to noise ratio

As a result, found that the sidelobe cancellation count on the variation of the phase center of the auxiliary antenna concerning the phase of the main antenna [1, 42].

4.1.4 Sidelobe blanking

The working principle of the sidelobe blanking method is simple and can be implemented easily leading to an advantage to the method [1, 39], sidelobe cancellation, and sidelobe blanking methods are similar to each other and work to affect the pulse interference using a low implementation ratio [39]. The sidelobe blanking and the system are completely independent technologies, the only difference between them and the sidelobe cancellation system at the track of signal processing [39]. The working principle of the sidelobe blanking method is comparing the amplitude of the echo signal received by the main channel with the amplitude received by the auxiliary channel, then to remove the interference the selection method will be used [?, 1]. The sidelobe blanking method will be effective only for pulse interference using a low implementation ratio if used in the case of clutter interference with a high implementation ratio, while the main lobe will be closed [39]. In the case of adding an auxiliary and receiving channel to the radar system, the output signals will be fusion processed, then the interference signal will be no more affect the radar operation, it can also process the interference coming from neighboring radars that operating at the same frequency band with great efficacy [19]. Figure 13 illustrates the block diagram of sidelobe blanking contains:

- Main channel which contains of main lobe with high gain and sidelobes with low gain,
- Auxiliary antenna using a low omnidirectional antenna that carries a gain is better than sidelobe gain but at the same time will be lower than main lobe gain,
- Transceiver antenna, Receivers, and Comparators [19].

Its working principle is as follows: If the comparator receives a signal with a main channel amplitude greater than the auxiliary channel, will be concluded that the signal entered from the main lobe and the gate circuit will transmit the signal received from the main channel to the next step in the signal processing procedure. But if the comparator receives a signal with an auxiliary channel amplitude greater than the main channel, will be sidelobe jamming. The gate control mechanism closes the circuit, so blocking the jamming signal entering the system from the sidelobe by using the detection of the target echo signal of the main channel [19].

4.1.5 Monopulse Angle Measurement Technology

Current radar systems make extensive use of monopulse technology, but with the evaluation of jamming technique the electromagnetic environment surrounding monopulse radars has become more complex due to the variety of intentional and inadvertent jamming tactics. The working principle of the monopulse angle measurement method based on the returned radar echo signal has been received by many antennas all simultaneously (at the same time). The aim is to focus on measuring the angle and azimuth information of the target this process is done by making a comparison between the amplitude and the phase of the received echo signal at each antenna. It's a more common method that is used to measure the azimuth in radar signal processing, also effective in angle jamming. In comparison with other techniques monopulse angle measurement is the more complex in building and performance technique [39].

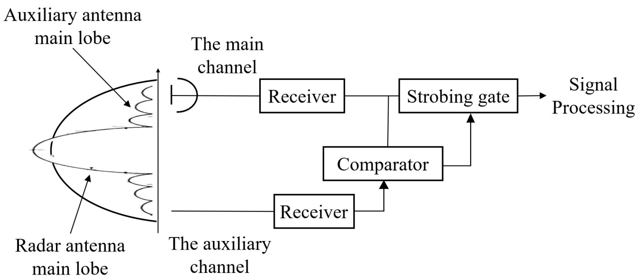

Figure 13**.** Schematic diagram of sidelobe blanking [43].

4.2 Anti-jamming Technology Based on Radar Transmitter

Figure 14 below shows the anti-jamming techniques based on radar transmitters that will be discussed in this section [1]. These techniques focused on active antijamming for the main lobe, and all will explained below [39]:

4.2.1 Frequency Agility Technology

Frequency agile is one of the most popular types of radar working to effect narrowband blocking jamming, while on broadband is inefficient. The frequency-agile radar transmitting pulses The carrier frequency of these pulses could be varied within the determined frequency range or varied randomly so that when the working frequency has been jammed, frequency agile radar can rapidly set a new frequency to counter the jamming [39]. The working of pulse-to-pulse frequency agile radar was discussed and focused on coherent signal processing. The phase difference caused by frequency agile radar has been measured using the Doppler profile. which has proposed a coherent signal processing method dependent upon minimum entropy to fix the phase difference [44]. Another approach was proposed that used a bank of matched filters working on removing the phase difference of the agile radar, to avoid jamming frequency agile radar should have a broad range of frequencies [45].

4.2.2 Frequency diversity

Frequency diversity works by dividing the radar operation frequency into different frequency bands, all these bands are working together simultaneously will leads to increasing the bandwidth of the frequency diversity. So, the bandwidth of frequency diversity is greater than the aiming jamming thus, the other diversity frequency bands(channels) will continue working normally. The process of expansion of the diversity bandwidth will force the jammer to expand the jamming's bandwidth, at the same time this will lead to a decrease in the jamming's power spectral density and increase the effectiveness of radar anti-jamming [1, 39]. The effectiveness of radar anti-jamming could be increased when using frequency diversity and single frequency radar signals, therefore this will provide both reducing the probability of detecting radar signals being the enemy and increasing the effectiveness of radar anti-jamming. Figure 15 illustrates the block diagram of frequency diversity [39].

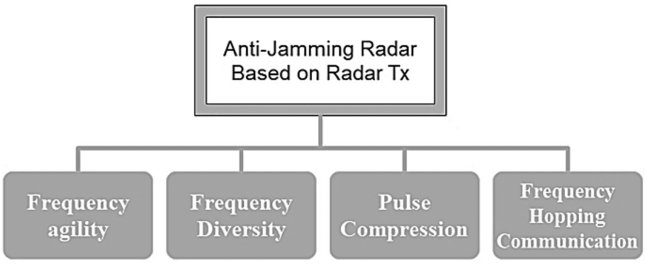

Figure 14. Types of radar anti-jamming techniques based on radar transmitter..

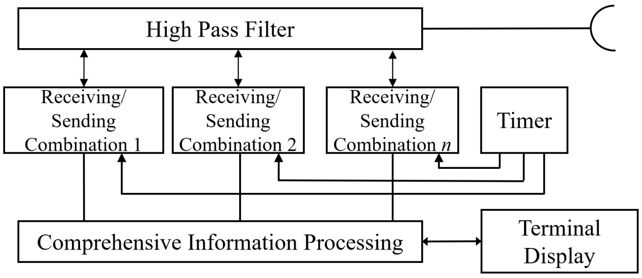

Figure 15. Block diagram of frequency diversity [32].

4.2.3 Pulse Compression Technology

The pulse compression method is a key radar signal processing technique that is used to resolve the trade-off between radar range and range resolution effectively. The working principle is as follows: transmitting a pulse with a larger pulse width that will achieve the ideal range, and compressing the echo signal to achieve the ideal range resolution. This technology (pulse compression technology) is most important in radar anti-jamming strategy, which focuses on suppressive jamming, and also has a specific anti-deception ability. Because of that, it's widely used today for radar signal processing. Figure 16 shows the system block diagram of pulse compression [39].

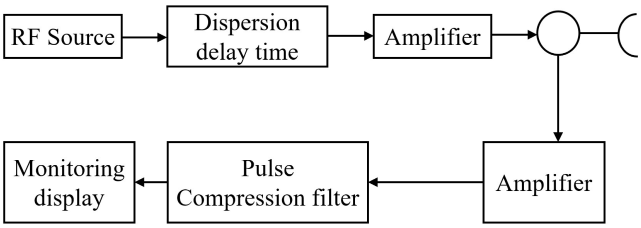

Figure 16. Block diagram of pulse compression technology [32].

A new framework has been proposed to avoid jamming by selecting frequencies. The frequency selection process can also be used for jamming devices to get strong and overall suppression over radars. To avoid the repeater jammer waveform parameters will be used because the repeater jammer's working principle is analyzing the radar parameters and then retransmitting the false parameters to the radar, these parameters like carrier frequency, the shape of pulses, pulse duration time, etc [46].

4.2.4 Frequency Hopping Communication Technology

The frequency hopping communication method works by using a series of pseudo-random sequences that aim to adjust the carrier center frequency for signal modulation. These sequences allow the carrier frequency to jump regularly or irregularly within a band of frequencies [1]. Using this method in a radar system will give:

- powerful anti-jamming capability,
- Provide communication with high-speed, continuous, and infrequent hopping carrier,

These properties make the process of detection and jamming by enemies more complex. By continuously varying the frequency of the radar's carrier signal, the impact of jamming signals could be avoided using frequency hopping communication technology. For jamming to affect a frequency hopping system, the jamming signal's frequency must exactly match that of the radar carrier signal at a particular moment. Nowadays, nearly all radar systems are equipped with frequency-hopping communication capabilities. Figure 17 illustrates the block diagram of the frequency hopping communication method [39]. A new approach is proposed to enhance the low recognition rate of airborne radar by a theory of identification ability applied to inspect a series of uniformly distributed design criteria for frequency hopping, optimizing the frequency and frequency range [47].

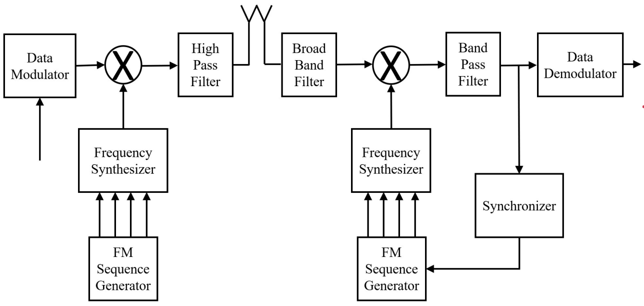

Figure 17. Schematic diagram of frequency hopping communication technology [32].

4.3 Anti-jamming Technology Based on Radar Receiver

If comparing anti-jamming techniques between radar receivers with the first kind we get:

- Antijamming technique based on radar receiver is more simple
- Economical
- Reasonable
- It's difficult to discover by the enemy jammers because it's a passive device.

The major anti-jamming techniques that are used on radar receivers are illustrated in Fig. 18 below and all will be explained below such as width limit narrow circuit, instantaneous automatic gain control, wide dynamic range receiver, etc. [39].

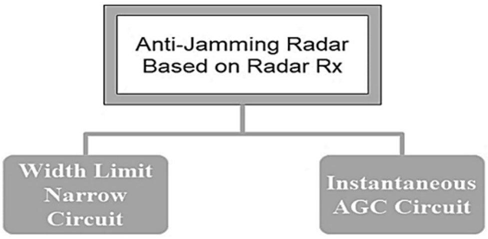

Figure 18. Types of radar anti-jamming techniques based on radar receiver.

4.3.1 Width-Limit-Narrow Circuit

The wide-limited-narrow circuit is designed to counteract wideband noise FM interference using a specific signal processing approach. The circuit working principle is passing the signal through a broadband amplifier circuit, followed by cascading it with a broadband limiter and a narrowband intermediate amplifier that matches the pulse width of the signal. Figure 19 illustrates the block diagram of a wide-limit narrow circuit [39].

4.3.2 Instantaneous Automatic Gain Control Circuit System

Instantaneous automatic gain control circuit (IAGC) classified as an anti-overload circuit, has been used in the IF section of the radar receiver. Its working principle to focus on blocking the IF amplifier overloads the radar receiver with jamming signals (interference signals) like similar amplitude interference, wide pulse interference, and low-frequency amplitude modulation interference. The operation of IAGC is like the operation of automatic gain control (AGC) but the difference is that IAGC is faster. To control the transmitting gain of the IF amplifier a negative feedback principle could be used by taking into account the changes in receiving interference signal, the block diagram of the IAGC circuit is shown in Fig. 20 [39].

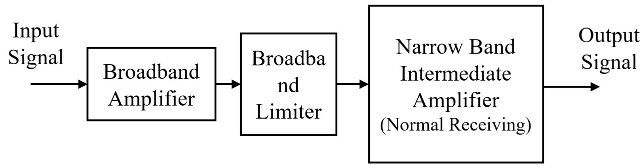

Figure 19**.** Block diagram of width-limit-narrow Circuit [32].

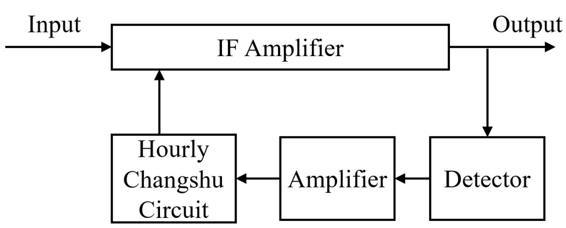

Figure 20**.** Block diagram of instantaneous automatic gain control circuit system [32].

4.4 Anti-jamming Technology Based on Signal Processing

The signals that enter into the radar receiver are processed using the knowledge of modern signal processing, this mechanism will greatly enhance the antijamming ability of the radar receiver. There are many anti-jamming techniques using signal processing as shown in Fig. 21 below will explained in detail, [39]:

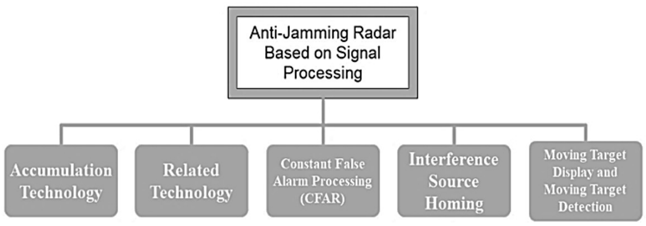

Figure 21**.** Types of radar anti-jamming techniques based on signal processing.

4.4.1 Accumulation Technology

The working principle of accumulation antijamming technology is to sample the signal received by the radar receiver over many periods and superimpose it. The power of the superimposed signal will be higher than the power of the jammer because the sampled signal is independent and irrelevant, the accumulation technology is classified into:

- Coherent accumulation, and Noncoherent accumulation [39]. Two methods have been proposed to improve the coherent accumulation method which is:
- The first method involved time and phase synchronization, which is dependent upon direct wave parameter estimation,
- The second method involved a weak target detection approach, which depended upon the agile waveform of long-time coherent accumulation.

This method works on simplifying the technical implementation of coherent accumulation. The major disadvantage is that it does not consider the estimation and analysis of errors in target parameter measurement and coherent accumulation [48].

4.4.2 Related technology

Relevant techniques are the most utilized in signal processing systems with a challenging environment. The related technology aims at measuring the received signal autocorrelation coefficient, by calculating the correlation between this received signal and the newly received signal after some time, otherwise, the correlation could be calculated between the received signal with the receiver's original signal or in other words after specific time interval computing the correlation between received signal and the local reference signal. These techniques will not only enhance the immunity of the radar system against jamming but also enable using the natural interference and the transmitted signals by the adversaries [39].

4.4.3 Constant False Alarm Processing (CFAR)

CFAR technique is the most used in contemporary radar. It aims to enable the radar to work normally under different jamming situations like rain clutter, ground clutter, etc., the constant false alarm processing technology used in the radar used two threshold processing schemes aims to enhance its ability to combat strong jamming interference and improve background display [39].

4.4.4 Moving Target Display (MTI) and Moving Target Detection (MTD)

To eliminate or remove interference from neighboring periods, the moving target display technology employs the difference in radar echo between stationary and moving targets, canceling out the echo of stationary targets effectively and retaining that of moving targets. This technology is known as moving target detection (MTD). It is often improved by adding cascading MTI (moving target display) filter banks based on FFT to improve clutter suppression capabilities. Both MTI and MTD technologies are effective in countering passive jamming [39].

4.4.5 Interference Source Homing (HOJ)

The jamming source-seeking technique is an effective anti-jamming method that uses missiles to route and destroy jamming signals from jammers. This approach, also known as a passive tracking jamming source, can prevent the enemy from easily jamming our radar [39].

5. Conclusion

Radar countermeasures obverse an increasingly complex EM spectrum, complex battlefield conditions, and increasingly advanced and complex countermeasures tactics; all of these are caused of the increased development of technology. Radar countermeasures must be involved to overcome the developed electronic countermeasure demands. This survey has highlighted the critical aspects of jamming and anti-jamming (countermeasures) techniques in the context of radar systems. Jamming specifies a significant threat to radar functionality by obstructing target detection and accurate parameter extraction. The survey has explored various radar jamming techniques, including mechanical and electrical jamming. The importance of understanding the environment and the capabilities of jammers has been emphasized to develop secure and effective anti-jamming systems. Moreover, the study has highlighted the dynamic relationship between jamming and anti-jamming technologies, where advancements in one domain drive advancements in the other. Future research and development efforts should focus on enhancing anti-jamming technologies to ensure the integrity and reliability of radar systems in modern warfare scenarios. Thus, in order to meet the needs of future battlefields, its necessary to have a deep comprehension of radar jamming and anti-jamming (countermeasure) methods.

Authors' contribution

All authors contributed equally to the preparation of this article.

Declaration of competing interest

The authors declare no conflicts of interest.

Funding source

This study didn't receive any specific funds.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] M. Aziz, A. Maud, and A. Habib, "Reinforcement learning based techniques for radar anti-jamming," *IEEE: Int. Bhurban Conf. Appl.*

Sci. Technol. IBCAST 2021, p. 1021–1025, 2021. [Online]. Available: https://doi.org/10.1109/IBCAST51254.2021.9393209

[2] M. Aref, S. Jayaweera, and E. Yepez, "Survey on cognitive anti-jamming communications," *IET Commun.*, vol. 14, no. 18, p. 3110–3127, 2020. [Online]. Available: https://doi.org/10.1049/iet-com.2020.0024

[3] A. Y. Rahmawati, "Communications," *communications, radar and electronic warfare, 2020*, 2020.

[4] , "An introduction to electronic warfare; from the first jamming to machine learning techniques," no. 1, 2017.

[5] S. Bhatia, K. Sharma, K. Chaudhary, and D. Singh, "Signal jammer and its applications," *International Journal of Electrical and Electronics Research*, vol. 3, no. 2, p. 463–467, 2015. [Online]. Available: www.researchpublish.com

[6] A. Pardhasaradhi and R. R. Kumar, "Signal jamming and its modern applications," *int. Journal of Science and Research(IJSR)*, vol. 2, no. 4, pp. 429–431, 2013. [Online]. Available: https://doi.org/10.21275/IJSRON2013808

[7] K. Khan, S. Ali, and M. Saif, "Fm radio jammer," 2019. [Online]. Available: https://doi.org/10.13140/RG.2.2.20488.47364

[8] A. Y. Rahmawati, "Fundamental principles of radar," vol. 89, pp. 397–407, 2020.

[9] G. Hatem, "Design and implementation of smart processor for performance enhancement of radar," *Canadian Journal of Civil Engineering*, 2023.

[10] M. A. Richards, J. A. Scheer, and W. A. Holm, *Principles of Modern Radar: Basic principles*. The Institution of Engineering and Technology, 2010. [Online]. Available: https://doi.org/10.1049/SBRA021E

[11] I. Luc, E. Jean-François, M. Jacques, and Y. Joe, "New approach of deployment of the multi-static radars based on an aperture angle and the probability of false alarm," *, Int. J. Eng.*, vol. 36, no. 9, p. 1589–1596, 2023. [Online]. Available: https://doi.org/10.5829/ije.2023.36.09c.01

[12] S. Li and B. Li, "Comparison of the radar receiver anti-jamming circuits performance," *World J. Eng. Technol*, vol. 5, no. 04, p. 152–158, 2017. [Online]. Available: https://doi.org/10.4236/wjet.2017.54b016

[13] H. Wang, B. Chen, and Q. Ye, "Design of anti-jamming decision-making for cognitive radar," *IET Radar, Sonar Navig*, vol. 18, no. 3, p. 514–531, 2023. [Online]. Available: https://doi.org/10.1049/rsn2.12497

[14] NAWCWP, "Electronic warfare and radar systems engineering handbook 2013," no. 4, p. e02433, 2013. [Online]. Available: https://doi.org/10.1016/j.cscm.2023.e02433

[15] K. RAMAKRISHNA and T. S. KUMAR, "Advanced mobile signal jammer for gsm , cdma and 3g networks with prescheduled time duration using arm7 tdmi processor based lpc2148 controller," *Int. Journal of Scientific Engineering and technology Research*, vol. 03, no. 30, p. 5929–5932., 2014. [Online]. Available: https://ijsetr.com/uploads/312654IJSETR2675-1044.pdf

[16] S. Wategaonkar, V. Bhivsane, and S. Kodgire, "Design and implementation of cell phone jammer by using microcontroller," *Advance Research in Analog and Digital Communications*, p. 15–19, Mar. 2024. [Online]. Available: https://doi.org/10.46610/ARADC.2024.v01i01.003

[17] E. Ataro, D. Starovoytova, and M. Sitati, "Design and testing of mobile-phone-detectors," *Innovative Systems Design and Engineering*, vol. 7, no. 9, 2016. [Online]. Available: https://www.iiste.org/Journals/index.php/ISDE/article/view/32979

[18] N. Nkordeh, I. Lawson, F. Idachaba, and I. Bob-Manuel, "Design and implementation of a dual band mobile phone jammer," *Lect. Notes Eng. Comput. Sci*, vol. 1, p. 119–123, 2016. [Online]. Available: https://www.academia.edu/download/94814523/WCECS2016_pp119-123.pdf

[19] G. Tang, Y. Cai, R. Gan, and Y. Zhao, "Techniques and system design of radar active jamming," *Springer*, 2023.

[20] "radar and electronic illustrated collection of definitions and formulas, (n.d."

[21] A. Okuyucu, "Effects of jamming on radars," 2000. [Online]. Available: https://doi.org/https://scholar.afit.edu/etd/4837

[22] Y. Wu, B. Wang, K. Liu, and T. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE journal on selected areas in communications*, vol. 30, no. 1, p. 4–15, 2012. [Online]. Available: https://doi.org/10.1109/JSAC.2012.120102

[23] M. Aref and S. Jayaweera, "A novel cognitive anti-jamming stochastic game," *2017 Cogn. Commun. Aerosp. Appl. Work. CCAA*, p. 1–4, 2017. [Online]. Available: https://doi.org/10.1109/CCAAW.2017.8001605

[24] K. Gavouchidis and D. Efstathiou, "a survey on jamming and friendly jamming techniques," *Far East J. Electron. Commun*, vol. 25, p. 1–36, 2022. [Online]. Available: https://doi.org/10.17654/0973700622001

[25] L. Xiao, D. Jiang, D. Xu, H. Zhu, Y. Zhang, and H.V., "Two-dimensional antijamming mobile communication based on reinforcement learning," *IEEE Trans. Veh. Technology*, vol. 67, no. 10, p. 9499–9512, 2018. [Online]. Available: https://doi.org/10.1109/TVT.2018.2856854

[26] C. Chen, M. Song, C. Xin, and J. Backens, "A game-theoretical anti-jamming scheme for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, p. 22–27, 2013. [Online]. Available: https://doi.org/10.1109/MNET.2013.6523804

[27] Q. Wang, K. Ren, P. Ning, and S. Hu, "Jamming-resistant multiradio multichannel opportunistic spectrum access in cognitive radio networks," *IEEE Trans. Veh. Technology*, vol. 65, no. 10, p. 8331–8344, 2016. [Online]. Available: https://doi.org/10.1109/TVT.2015.2511071

[28] S. Hanbali and R. Kastantin, "A review of self-protection deceptive jamming against chirp radars," *International Journal of Microwave and Wireless Technologies*, vol. 9, no. 9, p. 1853–1861, 2017. [Online]. Available: https://doi.org/10.1017/S1759078717000708

[29] X. Pan, W. Wang, D. Feng, Q. Fu, and G. Wang, "Repeat jamming against lfm radars based on spectrum-divided," *IET International Radar Conference*, p. D0490, 2013. [Online]. Available: https://doi.org/10.1049/cp.2013.0363

[30] X. Chen and B. Chen, "Anti-jamming approach based on radar transmitted waveform matching," *EURASIP J. Adv. Signal Processing*, vol. 2021, no. 1, p. 59, 2021. [Online]. Available: https://doi.org/10.1186/s13634-021-00776-w

[31] S. Zhao, Y. Zhou, L. Zhang, Y. Guo, and S. Tang, "Discrimination between radar targets and deception jamming in distributed multiple-radar architectures," *IET Radar, Sonar Navigation*, vol. 11, no. 7, p. 1124–1131, 2017. [Online]. Available: https://doi.org/10.1049/iet-rsn.2016.0540

[32] S. Gong, X. Wei, X. Li, and Y. Ling, "Mathematic principle of active jamming against wideband lfm radar," *Journal of systems engineering and electronics*, vol. 26, no. 1, p. 50–60, 2015. [Online]. Available: https://doi.org/10.1109/jsee.2015.00008

[33] J. Geng, B. Jiu, K. Li, Y. Zhao, H. Liu, and H. Li, "Radar and jammer intelligent game under jamming power dynamic allocation," *Remote Sens.*, vol. 15, no. 3, p. 581, 2023. [Online]. Available: https://doi.org/10.3390/rs15030581

[34] J. Wei, Y. Wei, L. Yu, and R. Xu, "Radar anti-jamming decision-making method based on dddpg-maddpg algorithm," *Remote Sensing*, vol. 15, no. 16, p. 4046, 2023. [Online]. Available: https://doi.org/10.3390/rs15164046

[35] C. Feng, X. Fu, J. Dong, C. Zhao, H. Chang, P. Lang, and T. Pan, "A radar anti-jamming strategy optimisation based on stackelberg game," *IET Radar, Sonar Navig.*, vol. 17, no. 8, p. 1248–1258, 2023. [Online]. Available: https://doi.org/10.1049/rsn2.12416

[36] J. Kim, Y. He, and H. Park, "Algorithms for nonnegative matrix and tensor factorizations: A unified view based on block coordinate descent framework," *Journal of global optimization*, vol. 58, no. 2, pp. 285–319, 2014. [Online]. Available: https://doi.org/10.1007/s10898-013-0035-4

[37] Z. Zhao and M. L. J. Yuan, "Research on adaptive waveform optimization design of anti-jamming radar," *J. Phys. Conf. Ser.*, vol. 1650, no. 2, p. 022111, 2020. [Online]. Available: https://doi.org/10.1088/1742-6596/1650/2/022111

[38] Q. Ling, P. Huang, D. Wang, H. Xu, L. Wang, X. Liu, G. Liao, and Y. Sun, "Range deception jamming performance evaluation for moving targets in a ground-based radar network," *Electronics*, vol. 12, no. 7, p. 1614, 2023. [Online]. Available: https://doi.org/10.3390/electronics12071614

[39] J. Liu and L. Liu, "Survey of radar anti-jamming technology and its research status," 2019. [Online]. Available: https://doi.org/

[40] K. Li, B. Jiu, H. Liu, and W. Pu, "Robust antijamming strategy design for frequency-agile radar against main lobe jamming," *Remote Sensing*, vol. 13, no. 15, p. 3043, 2021. [Online]. Available: https://doi.org/10.3390/rs13153043

[41] Q. Yan, B. Lin, and K. Wang, "Research on adaptive digital beam forming technology," *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China*, p. 446–450, 2018. [Online]. Available: https://doi.org/10.1109/ICCCBDA.2018.8386557

[42] N. Bloom and J. V. Reenen, "Analysis of side lobe cancellation algorithm for practical implementation," *NBER Work. Pap.*, vol. 89, 2013.

[43] M. Aslinezhad, A. Sezavar, and A. Malekijavan, “A noise-aware deep learning model for automatic modulation recognition in radar signals,” *Int. J. Eng. Trans. B Appl.*, vol. 36, no. 8, p. 1459–1467, 2023. [Online]. Available: https://doi.org/10.5829/ije.2023.36.08b.06

[44] R. Zhou, G. Xia, Y. Zhao, and H. Liu, “Coherent signal processing method for frequency-agile radar,” *2015 IEEE 12th Int. Conf. Electron.*, vol. 01, p. 431–434, 2015. [Online]. Available: https://doi.org/10.1109/ICEMI.2015.7494227

[45] C. Lin, R. Tian, Q. Bao, and Z. Chen, “Coherent integration method of frequency agile radar for target detection,” *2017 IEEE 6th Asia-Pacific Conf. Antennas Propagation, APCAP*, p. 1–3, 2017. [Online]. Available: https://doi.org/10.1109/APCAP.2017.8420601

[46] L. Ming and J. Zhang, “Study on anti-jamming frequency selection in radar netting,” *2016 2nd IEEE Int. Conf. Comput. Commun.*, p. 1781–1784, 2016. [Online]. Available: https://doi.org/10.1109/CompComm.2016.7925008

[47] f. wang, j. chen, j. zhang, and j. zhou, “lpid based criterion for airborne radar hopping frequency design,” *International Symposium on Signal, Image, Video and Communications (ISIVC), Tunis, Tunisia*, p. 364–368, 2016. [Online]. Available: https://doi.org/10.1109/ISIVC.2016.7894016

[48] Q. Lichang, K. Jia, and H. Guoxu, “Long-time integration of a multi-waveform for weak target detection in non-cooperative passive bistatic radar,” *J. Radars*, vol. 6, no. 3, p. 259–266, 2017. [Online]. Available: https://doi.org/10.12000/JR16137

How to cite this article:
Tabarek M. Makki, Ghufran M. Hatem, and Maytham K. Abbas, (20xx). 'A comprehensive survey on jamming and anti-jamming techniques in radar systems', Al-Qadisiyah Journal for Engineering Sciences, xx(yy), pp. 001- 010. https://doi.org/10.30772/qjes.xxxx.yyyyyy.zzzzz