CRPA for Anti-jamming Capability

Rajpal Singh , Prof (Dr.) Rajesh Bodade
Faculty of Communication Engineering, Military College of Telecommunication Engineering
Mhow, Indore, Madhya Pradesh - 453441
raistraj@gmail.com

***Abstract*— Controlled Reception Pattern Antennas (CRPAs) are designed to optimize the reception and processing of GPS/GNSS signals, minimizing interference while maximizing accuracy. By leveraging multiple antenna elements and advanced signal processing techniques, CRPAs achieve these objectives effectively. These systems are increasingly being adopted, particularly in the Defense sector. CRPAs are highly efficient in countering jamming and spoofing, as they dynamically adjust to mitigate such disruptive signals. To implement null-steering and beamforming techniques, it is essential to determine the direction of the interference or jammer. With the widespread use of GPS in defense equipment, ensuring reliable GPS performance in mission-critical operations, especially in jamming environments, is vital. As such, studying this technology within systems that can provide anti-jamming capabilities for GPS-enabled devices—such as drones, GPS receivers, target acquisition systems in firearms, tanks, and helicopters—is crucial.**

Keywords—CRPA; Beamforming; Beamsteering; Anti-jamming; Military, GPS, GNSS, Null steering

I. Introduction To GPS

The primary objective of all Global Navigation Satellite Systems (GNSS) is to provide accurate and reliable Positioning, Navigation, and Timing (PNT) information, sometimes referred to as Positioning, Velocity, and Timing (PVT). The set of these values at a given moment is called the almanac, which is acquired by the receiver. Two kinds of services provided by the Global Positioning System are Precise Positioning Service and Standard Positioning Service. The SPS is available to the general public, while the PPS is restricted to selected users, such as the U.S. Department of Defense (DoD). The GPS frequencies are as follows: L1 at 1575.42 MHz, L2 at 1227.6 MHz, and L5 at 1176.45 MHz. The PPS employs the P(Y)-code, designated for military purposes and authorized civilian users. This code is created by encrypting the P-code with a secret W-code, producing the Y-code. The Y-code is then modulated onto the L1 and L2 carriers, offering protection against spoofing. In contrast, the SPS employs the C/A (Coarse/Acquisition) code modulated on L1 or the CM/CL (Civil Medium/Civil Long) codes modulated on L2. GPS signals are transmitted by a network of orbiting satellites at an altitude of approximately 20,200 km.

Typically, GPS signals are transmitted at approximately 25 W (around 27 dBW when factoring in the satellite antenna gain of 13 dB). However, the received signal at a standard GPS receiver is much weaker, typically falling in the range of -155 to -160 dBW, well below the noise floor. Given the weak received signal strength, a hostile source equipped with a 3 dBi gain antenna can successfully jam a GPS receiver positioned as far as 100 km away, using a transmitter that operates with less than 50 W of power.

The reception of GNSS signals can be significantly disrupted by either unintentional or intentional interference, especially in military operational environments. Any substantial degradation in signal strength can result in reduced signal availability, diminished continuity, and lower positioning and timing accuracy. Consequently, additional protective measures are necessary to safeguard the weak GNSS signals (with received power levels around PRx ≃ -130 dBm at the Earth's surface) from potential high-power interference. Figure 1 illustrates the jammer-to-signal (J/S) ratio as a function of distance for different jammer power levels, ranging from 0.1 W to 100 W EIRP. The red lines in the figure mark the susceptibility threshold for different acquisition methods, including SPS and PPS, as well as for a GPS receiver utilizing advanced signal processing correlation and filtering techniques to recover the signal from the noise floor. [1]

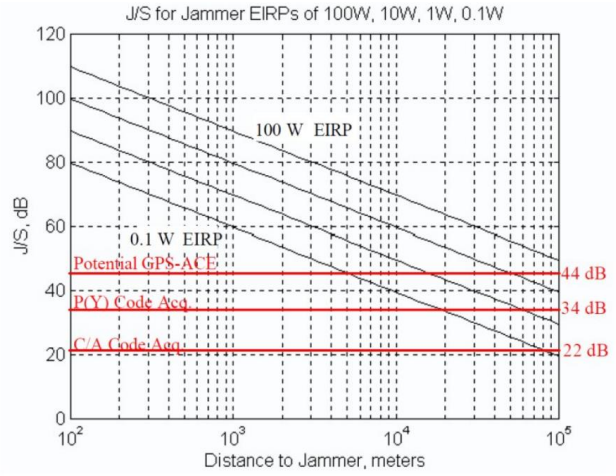

Fig. 1. Distance for various jammers EIRP levels versus Jammer to signal ratio (J/S) and vulnerability thresholds for different GPS signal reception methods (Adapted from [8])

Since GPS signals are typically below the noise floor of a standard GPS receiver, any signals detected above this noise floor are classified as jammers or interferers, which can then be further filtered. As a standard approach, fixed bandwidth front-end radio frequency (RF) filters are used to eliminate out-of-band jammers and general interference. For more effective filtering of continuous wave (CW) tone jammers, intermediate frequency adaptive notch filters can also be utilized. These two techniques generally provide jammer suppression in the range of 15 to 30 dB, which is sufficient to mitigate the impact of moderate power jammers located at least 10 km away (as referenced in Fig. 1). However, to address closer-range and/or high-power jammers, anti-jamming techniques beyond digital signal processing and frequency domain hardware filtering are required. Specifically, spatial filtering methods that actively manage the radiation and reception patterns of the GPS antenna need to be utilized.

II. CONTROLLED RADIATION PATTERN ANTENNA

A. *Introduction*

CRPAs leverage spatial diversity because satellite signals and jamming signals generally arrive from different directions, making them spatially distinct. Simply put, a CRPA functions as a spatial filter, isolating signals from specific directions while permitting signals from other directions to pass. To achieve this, instead of relying on a single antenna, a CRPA uses an array of antenna elements.

As shown in Fig. 2, imagine antennas labeled 1, 2, and so on. A signal arriving from a particular direction first reaches antenna 2, followed by antenna 1, and subsequently antenna M. For example, if the signal is a simple sine wave, the output from each antenna will feature the same sine wave but with different phase shifts, determined by the spatial configuration of the antenna array. The signal arrived at each Antenna is given by: [4]

$$x_m(t) = s_k(t).e^{-j.2\pi(m-1).dSin(\theta k)}$$

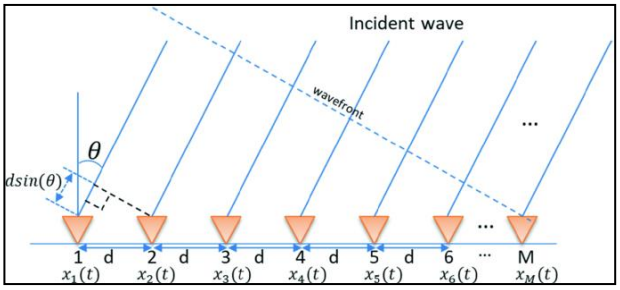

Fig. 2. Wavefront arrival on array of antenna and exploiting Direction Of Arrrival (DOA)(Adapted from [2])

B. *J/S levels using CRPA*

By employing multiple antenna elements that capture spatially diverse signals, the CRPA attenuates jamming signals through null-generation or null-steering, attenuating interference while simultaneously amplifying the reception of true signals through beamforming or beamsteering, as visually depicted in the diagrams above. An efficient approach to improve the robustness of GNSS receivers is the realization of a CRPA with M elements, as it allows for the adaptation of the antenna pattern, enabling the placement of spatial nulls in the direction of jammer signals.

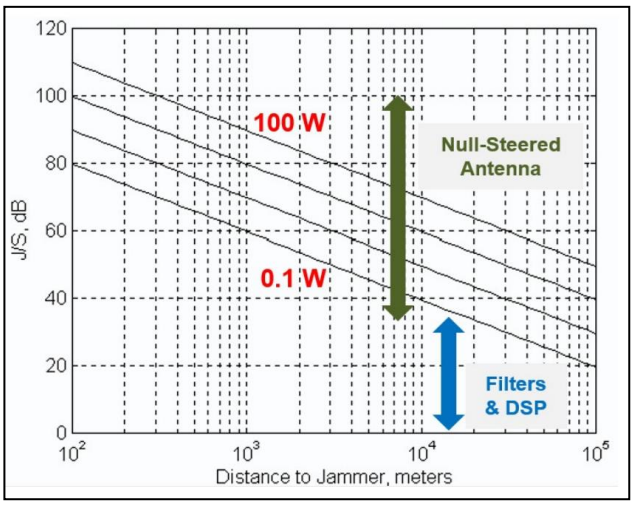

Fig. 3. Distance for various jammers versus Jammer to signal Ratio (J/S) and vulnerability thresholds for different GPS signal reception methods (Adapted from [8])

The dynamic null-steering method can boost jammer suppression by an additional 30–50 dB, significantly enhancing the CRPA anti-jam GPS system's ability to reduce the impact of nearby, high-power jamming sources, especially when compared to conventional GPS receivers. To illustrate the technique's effectiveness, the jammer-to-signal ratio can be graphed against the distance from the jammer, while factoring in the suppression effects from frontend filters (like Digital Signal Processing or DSP) alongside active null-steering. This graph clearly showcases the increased jamming resistance achieved through dynamic null-steering, emphasizing its critical role in improving overall suppression.

C. *Basic functioning of CRPA*

A standard Controlled Reception Pattern Antenna (CRPA) utilizes adaptive array techniques, incorporating an adaptive array of GPS antennas. The number of antenna array elements is calculated by the number of jamming signals the CRPA is designed to mitigate. Specifically, an array with N elements can counter up to N-1 jamming signals. In addition to the GPS antenna array, the system comprises of an Antenna Control Unit and a null-steering network—comprising components such as phase shifters and attenuators—to recognize jamming signals and fine-tune the array's radiation and reception patterns accordingly.

The CRPA operates by identifying the direction of jamming signals in real-time and dynamically fine-tuning the amplitude and phase of all array elements. This attenuates power reception from jamming sources while ensuring optimal reception of true satellite signals. The weight values of array elements are calculated through an optimization algorithm designed to attenuate jammer signal power at the combined output, ensuring the reception of true GPS signals via a designated "primary antenna."

The RF signals received by the array elements, $X_1(t)$ to $X_N(t)$, are combined based on their respective amplitude and phase weights, w_1 to w_{N-1}. This process generates the desired radiation and reception pattern, with nulls effectively steered toward the jammer directions. [5]

A typical CRPA is depicted below by a block diagram:

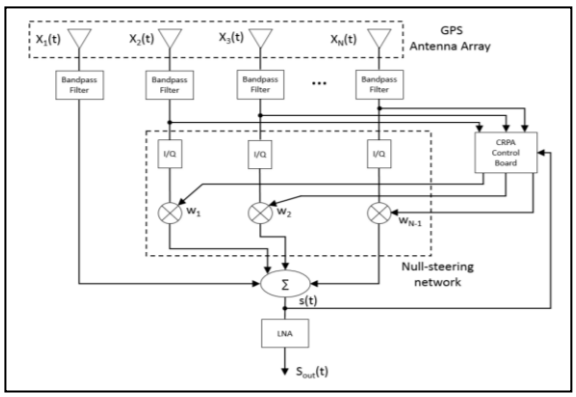

Fig. 4. Block Diagram for basic CRPA (Adapted from [9]).

For precise Positioning, Navigation, and Timing (PNT) information, it is vital to track signals from at least four different GPS satellites. To further reduce errors originating from various sources, tracking signals from more number of GPS satellites is highly desirable. Therefore, the ability to cancel certain types of interference through methods apart from spatial null steering would be highly advantageous.

D. Degree of Freeedom and jammers

As stated above, an array of 'N' number of antenna elements can defend against 'N-1' number of jamming signals. Thus, Degree of Freedom can be stated as N. This limits the number of jammers that can be nullified by CRPA and thus throttling one of the key performance parameter.

III. HARNESSINGH FREQUENCY AND TIME DOMAINS

A. Space-Time Adaptive Processing (STAP)

With this model, known as **S**pace-**T**ime **A**daptive **P**rocessing (STAP), the individual weight coefficient of each antenna element is substituted with a full finite impulse response (FIR) filter, featuring N time taps. The updated block diagram is shown in Fig. 5. [5] [6] Thus, the adaptive filter's total **number of degrees of freedom increases** to N × M, which provides more flexibility in cancelling interference signals in the same form factor of array size of N.

B. Space-Frequency Adaptive Processing (SFAP)

Frequency processing is mainly used to combat narrowband interference. In Controlled Reception Pattern Antennas (CRPAs), digital beamforming techniques are applied by combining signals from an antenna array. Space-Frequency Adaptive Processing (SFAP) creates nulls in both the spatial and frequency domains, allowing it to eliminate more than N-1 jammers, even when some are narrowband. However, the high computational complexity of Space-Time Adaptive Processing (STAP) or SFAP presents significant challenges for real-time software receiver deployment.

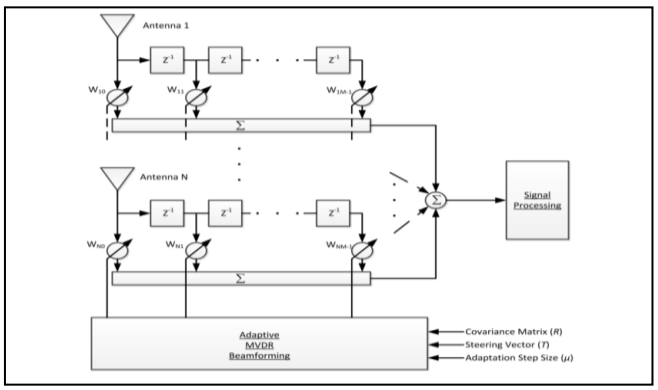

Fig. 5. Basic block diagram depicting MVDR beamforming algorithm in STAP (Adapted from [10]).

Various algorithms within Space-Time Adaptive Processing (STAP) and Space-Frequency Adaptive Processing (SFAP) have been developed for weight calculation. Some of these algorithms optimize specific criteria based on the known signal structure of the desired signal, such as maximizing the signal-to-interference ratio, minimizing mean square error, or reducing output power. On the other hand, algorithms like Minimum Variance Distortionless Response (MVDR) and Constrained Least Mean-Squares do not rely on prior knowledge of the signal structure. Instead, they focus on minimizing output power while adhering to specific constraints. These constraints can be set to form a beam in the direction of the satellite or to steer a null towards interference. The steering vector for the satellite's direction can be derived from satellite ephemeris and array calibration data, or alternatively, by utilizing carrier phase differences between the antenna array elements as a basis for modeling.

IV. TYPES OF CRPA ANTENNAS

There are various types of CRPA antennas used in military applications, each designed to meet specific operational requirements and on basis of capability, form factor and shapes. Few of the important classifications are listed below:

A. Fixed Beam CRPA

1) **Descrip*tion***: Fixed beam CRPAs utilize a pre-determined reception pattern, which offers a stable and simplified method of interference mitigation. The beam pattern is optimized for certain environments or missions but lacks dynamic adaptability.

2) **Usage**: These antennas are commonly employed in less complex scenarios where jamming threats are predictable, or the operational environment is stable. They are typically used in situations where electronic warfare capabilities are minimal or where cost-effectiveness is a key factor.

B. Adaptive Beamforming CRPA

1) **Description**: This is the most widely used type of CRPA in military applications. Adaptive beamforming CRPAs continuously monitor the signal environment and adjust their reception pattern in real-time. These antennas are equipped with algorithms that detect and respond to jamming signals, placing nulls in the direction of the interference while maintaining strong reception from satellite signals.

2) **Usage**: Adaptive beamforming CRPAs are employed in dynamic and contested environments where the threat of jamming is unpredictable or widespread. These systems are crucial for military aircraft, naval vessels, and ground vehicles operating in electronic warfare zones.

C. Hybrid CRPA

1) **Description**: Hybrid CRPAs combine the features of adaptive beamforming and fixed beam CRPAs, providing a blend of flexibility and stability. They can switch between a fixed reception pattern and adaptive modes, depending on the operational needs or threat level.

2) **Usage**: Hybrid CRPAs are used in versatile military platforms that require both long-term stability and adaptability to sudden jamming threats. These antennas are commonly integrated into platforms that operate in a variety of mission profiles, including intelligence, surveillance, and reconnaissance (ISR) missions.

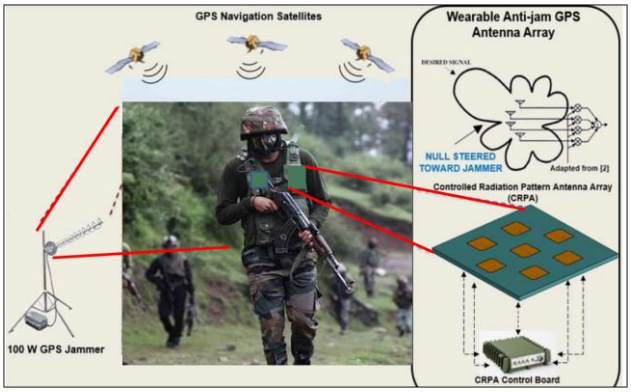

Fig. 6. artoon illustrating the GPS 100 W jammer and the wearable CRPA anti-jam solution. [9]

D. Wearable CRPA

1) **Description**: The human body presents significant constraints as a platform for an anti-jam antenna array, limiting its total size to less than 5 x 5 x 1 inches. Although compact, current Controlled Reception Pattern Antenna (CRPA) designs often rely on rigid, heavy, or thick dielectric substrates that lack essential characteristics for wearable systems, such as flexibility, conformability, and durability. To address this challenge, there is a pressing need for a flexible, conformal antenna—either externally mounted or integrated into textiles—that meets the demands of a wearable CRPA.

2) **Usage**: This can be a use case of on Foot soldier/ Infantry soldier leading missions in combat hostile environment. The cartoon illustrates the issue of GPS jamming and how a wearable CRPA anti-jam system can offer a solution in an operational environment for a dismounted Infantry soldier depicted in Fig 6.

V. Challenges and Advent of Technologies

A. Challenges in CRPA

1) **Form-factor**: It becomes very large for many smaller platforms like UAV, Drone, Infantry Soldiers to accommodate. This leads to trade-off, that is, if we reduce the M in order to reduce form factor, unfortunately, degree of freedom also gets reduced as antenna array number reduces.

2) **Beamwidths:** We know that the array aperture in the GPS application is typically on the order of a wavelength, two jammers may be relatively widely-spaced in terms of physical angle but closely-spaced in terms of beamwidths. Therefore, a single null may null out two jammers (or more depending on their locations). However, in GPS application, the no of antennas is small due to cost, size restrictions, power consumption, etc. Thus, attenuation of jammers solely through spatial-nulling consumes valuable degrees of freedom and thus limits AJ capability.

3) **Nulling of Satelite alongwith Jammer:** If jammer and a GPS satellite are closely-spaced in angle, the spatial null towards jammer may also null the gain of that GPS satellite rendering it useless. Again, due to the abovementioned small aperture challenge, a jammer and GPS satellite bearing may be reasonably widely-spaced in terms of physical angle but closely-spaced in terms of beamwidths.

4) **Testing CRPA.** Simulating random jammers with random power becomes challenging, thus testing in simulated hostile environment is resouce intemsive.

B. Scope with Latest Technologies

1) Use of preloaded Almanac and Satellite Ephemeris

- Alamanac: An almanac contains information about a satellite's orbit and status, which can help determine which satellites are visible when a receiver is powered on.
- **Almanac and Satellite Validation**: Spatial validation of satellites involves measuring the DOA and comparing them with the almanac to authenticate the location of satellites in the space. Upon powering up for the first time, the receiver acquires the almanac, and the time taken for this process is called the time to first fix (TTFF), also known as a Cold Start. When the receiver already has an estimate of the current time and position, along with a recent copy of the almanac data, it is referred to as a warm start.
- Satellite Ephemeris: It is a list of a satellite's location and velocity at specific times, calculated from observations. It's used to track a satellite's location in the sky.
- Almanac and First Fix: An almanac can help speed up the time it takes to get a first fix on a satellite by up to 15 seconds. It can pre-align the beam towards AI model identified Satellite loc.

2) Machine learning (ML) and artificial intelligence (AI) offer substantial potential for enhancing CRPA (Controlled Reception Pattern Antenna) systems by making them more adaptive, resilient, and accurate. Specifically, ML and AI techniques can improve CRPA performance by optimizing signal processing, interference mitigation, adaptive beamforming, and fault detection.

- **Challenge:** Traditional CRPA systems use algorithms like least mean squares or minimum variance distortionless response (MVDR) for interference suppression. However, these techniques might struggle to adapt to dynamic environments where interference types and sources change frequently.
- **AI/ML Solution**: Machine learning algorithms (especially deep learning models) can be trained on a large dataset of interference patterns and sources, allowing the system to learn the characteristics of different interference types (e.g., jamming or spoofing).
- **Data Collection**: Collect data on various types of interference (e.g., GPS jammers, spoofers, environmental noise) in different operational environments.
- **Model Training**: Train ML models, such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs), to recognize interference patterns. These models can be fine-tuned to recognize subtle interference signatures.
- **Real-Time Detection:** In deployment, the trained model processes incoming signals in real-time to classify interference sources and adapt the CRPA pattern accordingly.

VI. Conclusion

Controlled Reception Pattern Antennas (CRPAs) play a pivotal role in mitigating jamming and interference challenges in GPS-dependent systems, especially in defense applications. By leveraging adaptive beamforming and null-steering techniques, CRPAs significantly enhance the anti-jamming capabilities of GNSS receivers, ensuring accurate Positioning, Navigation, and Timing (PNT) even in contested environments. The integration of advanced methodologies like Space-Time Adaptive Processing (STAP) and Space-Frequency Adaptive Processing (SFAP) has further expanded the degrees of freedom in CRPA systems, enabling them to counter a larger number of threats. Despite these advancements, challenges such as reducing the form factor, improving nulling precision for closely-spaced satellites and

jammers, and enabling real-time testing in simulated environments remain significant. The incorporation of machine learning and artificial intelligence offers promising solutions to these challenges, paving the way for smarter, more adaptive CRPA systems. Future research should focus on refining these technologies to enhance performance while addressing constraints in size, cost, and computational requirements. [5] [6]

REFERENCES

[1] Kaplan, E. D., & Hegarty, C. J. (2005). Understanding GPS: Principles and Applications. Artech House.

[2] Skolnik, M. (2008). Introduction to Radar Systems. McGraw-Hill.

[3] Misra, P., & Enge, P. (2001). Global Positioning System: Signals, Measurements, and Performance. Ganga-Jamuna Press.

[4] Ward, N. (2006). Controlled Reception Pattern Antennas (CRPA) for GPS. IEEE Aerospace Conference Proceedings.

[5] Van Trees, H. L. (2002). Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory. Wiley-Interscience.

[6] Rao, B. (2010). Global Navigation Satellite Systems and Their Applications. McGraw Hill Education.

[7] Tsui, J. B. Y. (2005). Fundamentals of Global Positioning System Receivers: A Software Approach. Wiley.

[8] Keller, Steven D, (2016). Anti-Jam GPS Antennas for Wearable Dismounted Soldier Navigation Systems, US Army Research Laboratory, ATTN: RDRL-SER-M, 2800 Powder Mill Road ,Adelphi, MD 20783-1138

[9] Mingjie D, Xinjian P, Fang Y, Jianghong L. Research on the technology of adaptive nulling antenna used in anti-jam GPS. Proc. of 2001 CIE International Conference on Radar; 2001 Oct. p. 1178–1181.

[10] Chen, Yu-Hsuan, Jyh-Ching Juang, Jiwon Seo, Sherman Lo, Dennis M. Akos, David S. De Lorenzo, and Per Enge. 2012. "Design and Implementation of Real-Time Software Radio for Anti-Interference GPS/WAAS Sensors" Sensors 12, no. 10: 13417-13440. https://doi.org/10.3390/s121013417