Study of the Effect of Barrage and Deception Jamming on a Radar System along with their Mitigation Technique

Surendra Khadka[1], Dr. M. S. Anuradha[2], Ch. Padmasree[3]

[1]M.Tech. Students, Andhra University College of Engineering, Sainbu-bhainsepati, Lalitpur, Nepal

[2]HOD, Department of ECE, Andhra University College of Engineering (women), Visakhapathnam, Andhra Pradesh, India

[3]Lecturer, Andhra University College of Engineering (women), Visakhapathnam, Andhra Pradesh, India

Abstract: ***The main idea of radar jamming is to minimize the (signal to interference plus Noise ratio) SINR value of the return radar echo as far as possible and also load radar screen with excessive fake target so that target detection ability of radar is voided. Here we present two jamming algorithm: Barrage and Deception jamming for surveillance radar with comparative study and also their mitigation techniques. The jamming mitigation techniques used in this text are space time adaptive processing (STAP) and Power stagger pulse with differential receiver. STAP, is based on the idea of designing a two-dimensional (space and time) filter that maximizes the output signal-to-interference noise ratio. On the other hand Power stagger pulse with Differential receiver technique is used to negate the effect of deception jamming by canceling the common jamming signal.***

Keywords: ECM, Barrage jamming, Deception jamming, SINR, SNR, STAP, AGC.

1. Jamming Introduction

1.1 Barrage plus Noise jamming

Jammer transmits random noise plus signals of suitable frequency and power towards the radar receiver, in order to increase the noise floor of the receiver and at same time making interference with radar signal. Such that the radar cannot extract the information about target using return echo [4]. As figure1 illustrates, the average amplitude of the target echo is overwhelmed by noise so it is no-more distinguishable. Another way of expressing the same is, the signal to noise ratio at the input is lowered to a level beyond which the receiver cannot extract intelligence.

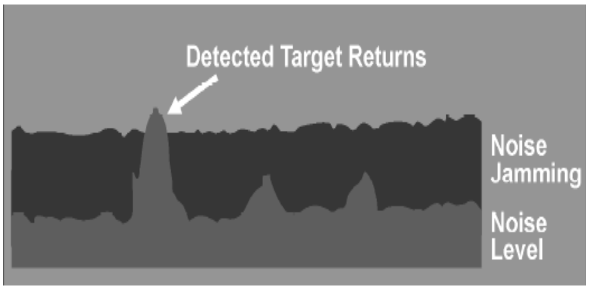

Figure 1: Illustration of Noise jamming

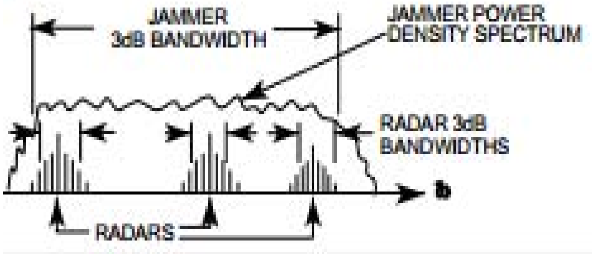

Figure 2: Jammer's and radar spectral view.

Barrage jammers attempt to increase the interference level across the entire radar operating bandwidth. Consequently, this lowers the receiver SINR, and in turn makes it difficult to detect the desired targets. Barrage jamming is the jamming of multiple frequencies at once by a single jammer with the intention of interfering the radar signal. Especially design to jam frequency agile radar. However jamming effect is limited because this technique requires the jammer to spread its full power in wide range of frequency. Larger the frequency band of jammer less is the jamming effectiveness.

The combine use of Barrage and Noise signal are used to mal-function the Radar more effectively. The signal to interference plus noise ratio (SINR) is one of the parameter to indicate the jamming performance of the receiver [1]. More we minimize the value of SINR at radar receiver more effective will be the jamming.

1.2 Deception Jamming

Deception jamming systems are designed to inject false information into the victim radar to deny critical information on target azimuth, range, velocity, or a combination of these parameters [6].Deception jammers sense incoming radar signals and generate replicas that simulate target echoes in order to confuse radars, hindering the ability of radar to indentify true targets by these false targets. False target generation (FTG) is a commonly used form of deception jamming.

The radar signal is replicated and delayed to create a range offset. The delayed waveform is transmitted at the next expected arrival of the radar signal and is seen as an actual target during the correlation process [11].

These techniques introduce a change in the range by introducing the delay to the echo signals, velocity can be altered by introducing Doppler shift on radar pulse, and direction estimation can be altered by injecting the jamming signal on the side lobe of radar receiving antenna, or may distract the radar beam from target by using inverse gain jamming technique. Range gate pull over(RGPO), and velocity gate pull over (VGPO) are main technique basically used to distract the radar from the target especially to distract the tracking radar. Here these technique use stair case approximation to free the target that was initially locked on the radar vision.

1.3 Inverse gain jamming:

Inverse gain is a angle deception jamming in which number of false target is created for every bearing in order to make radar confusion.

The idea is to use a *strong* jamming replica when the radar beam points off target and a *weak* jamming signal when the radar beam is on target [12]. Doing so radar receiver continuously receives the echo from target for every scan angle. Due to inverse gain, the searching radar beam will deviate from real target as the signal strength coming from jammer is strong than real target. So the tracking ability of radar is violated. In a simple form inverse gain is an 'angle deception' kind, because the radar is still able to measure range correctly and it is the angle indicator which shows the wrong readings [7].

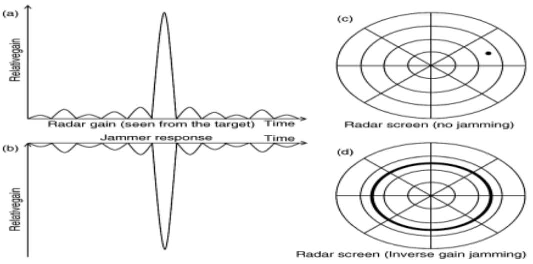
(a)
Relativegain
Radar gain (seen from the target)
Time
Jammer response
Time
(b)
Relativegain
(c)
Radar screen (no jamming)
(d)
Radar screen (Inverse gain jamming)

Figure 3: Inverse gain jamming configuration.

2. Jamming Mitigation Techniques:

2.1 Barrage plus Noise jamming: STAP Radar.

Space-time adaptive processing, or STAP, is based on the idea of designing a two-dimensional (space and time) filter that maximizes the output signal-to-noise ratio, thereby selectively Nulling clutter and jamming returns while at the same time retaining the target signal [2].

A space-time adaptive processing combines receive beam-forming in the spatial dimension and Doppler filtering in the temporal dimension to achieve the specific filter response. The filter is formed by simultaneously combining the signals received on multiple elements of an antenna array and multiple pulse-repetition intervals of a coherent character. The antenna elements provide the filter's spatial dimension and the pulse-repetition intervals provide the temporal dimension. STAP filters the raw data called snapshot in both space and time dimension in order to collect weak echo signal leaving behind clutter and jammer signal. In a simple sense beam is formed with chosen spatial and frequency directions matched to the target signal, and possessing nulls in the directions and frequencies of adaptively sensed interferers [4].

The radar transmits a train of M coherent pulses simultaneously from each element. The echoes from potential targets (clutter and jammer) are collected at each of the N elements of an antenna array. Separate receiver chains are attached to each of the array elements. The received signals are sampled at a series of L successive ranges (i.e., distances) also referred to as range gates. STAP processing is applied to the $M \times N$ matrix of samples collected at each range gates. The collected sample signal after proper weighting and superimposition gives desired filter response. The main task here is to find beam forming weight.

In STAP design beam forming weights are computed from radar returns containing information on the spatial and temporal characteristics of the interference. Two weights especially used for STAP processing are target steering vector and interference covariance matrix. Target steering vector specify the match filter parameter for received signal so that the target signal SNR value is increased. For each suspected target, a target steering vector must be computed. These suspects target come from rough approximation in covariance matrix manipulation [3]. The target steering vector collects the echo with high gain for approximated target.

The interference covariance matrix must compute for all range bins. The interference covariance matrix S can be computed from the return of fixed number of training sequences especially for adaptive STAP. The covariance matrix for a particular range bin can be expressed as $\mathrm{S}=\mathrm{Y}*.Y^{T}$

Here y is a data cube for a particular range bin. The covariance matrix represents the degree of correlation across both antenna array inputs and coherent pulse .The main intention here is to characterize undesired signals and create an optimum filter to remove them. The undesired signals include noise, clutter and jammer [9]. The optimal adaptive weight vector **w** for a given steering vector **t** is related to the interference covariance matrix **S** through the relation

$$\mathbf{w}=\mathbf{t}\,\boldsymbol{S}^{-1}$$

The beam-forming operation is just a matrix-vector multiplication,

$$\mathbf{z} = w^{T}\mathbf{y}$$

where **y** is the input data for a specific range gate. Where **z** is a complex scalar, which is then fed into the detection threshold process. Where decision is made based on the result of this signal processing output.

In special case when jammer and target align in same direction then STAP technique will not work because it forms a null in direction of target. Hence the target is masked by the null of STAP processor. This is the main drawback of STAP mitigation techniques.

2.2 Deception jamming mitigation: Power Stagger pulse with differential receiver

In stagger pulsed radar system we transmit pulse with stagger power, ie transmitted power level vary from pulse to pulse. Consequently the received radar echo pulse strength will also vary from pulse to pulse. The change of radar transmission power on a pulse-to-pulse basis allows radar to differentiate between returns from its own transmissions and returns from other radar systems, jammer and interference [10]. This is one technique to distinguish jamming signal from radar echo. Second or main idea of power stagger pulse is described as follow. Actually the jammer transmission power is almost constant in real scenario. This case can be used to mitigate the jamming effect.

As we transmit the radar signal with stagger, i.e power changing from pulse to pulse, the corresponding echo power will also change so accordingly, So at radar receiver which accepts differential input, i.e if we subtract the received echo for a pulse with its previously arrived pulse then due to constant jammer power the jammer signal get canceled and only the echo signal remain. From which we can extract the target information.

This techniques works well if the jammer is in rest or in slow motion because here we need is constant jamming power arriving at radar. But if the jammer is moving relatively with high speed then the jamming power at radar receiver will not be constant. And this mitigation technique works no more. In order to address these problem Automatic gain control system is introduced in radar receiver. Such that receiver provide gain to the received signal depending upon its time of arrival [5]. Hence this can mitigation distance-power variation problem. And hence help to maintain the jamming power constant despite of its motion. Actually AGC compensate the effect of free space propagation loss.

3. Simulation Result

The simulations were implemented in MATLAB 2014b

3.1 Barrage jamming

Table 1:Radar specification for Matlab simulation

Pulse width	*0.33*	*µs*
PRF	*30*	*Khz*
Carrier freq.	*10*	*Ghz*
Sampling freq.	*6*	*Mhz*
Tx. Power	*5.2*	*KW*
Tx.ant. gain	*20*	*-*
SNR (req)	*4.99*	*-*

Table 2: Configuration of radar, jammer and target

	Position (m)	*Range*	*Relative angle*	*Relative speed(m/s)*
Radar	(0,0,0)	-	-	0
Target	(3000,1000,1000)	3316	(18,17)	17
Jammer	(2500,2000,1000)	3354	(39,17)	0

Jammer power=100w.
Jammer freq=(9.9-10.1)GHz

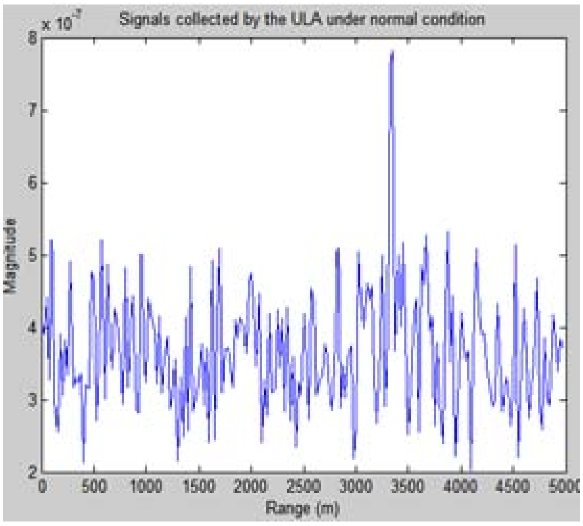

Figure 4: Waveform received by radar during normal condition

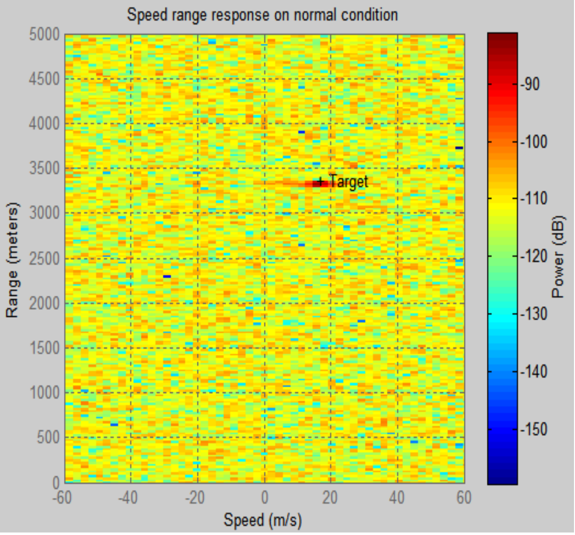

Figure 5: Range Speed response during normal operation

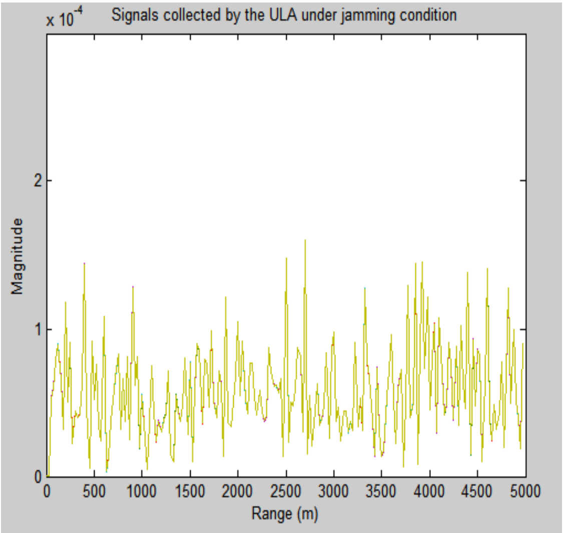

Figure 6: Waveform received by radar receiver during jamming condition.

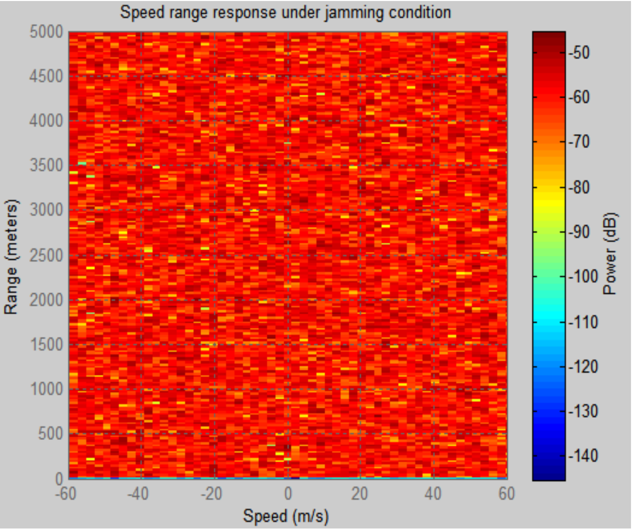

Figure 7: Range Speed response at radar receiver during Barrage jamming condition.

Barrage jamming Mitigation (STAP):

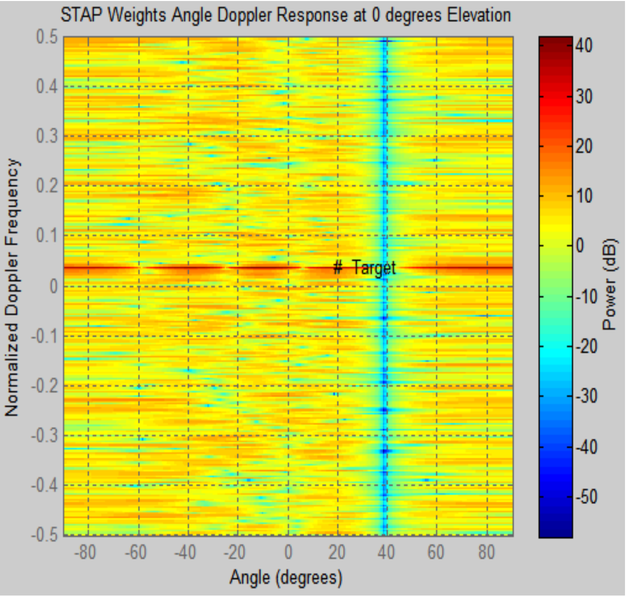

Figure 8: STAP Nulling at the direction of jamming.
(jammer is at an angle of 39 degree)

Figure 4 shows the waveform received by radar during normal condition. The spike at range of 3300 m refers the target return echo. Figure 5 is representation of same in Speed-Range domain. Figure 6 shows the received waveform under barrage jamming condition. Here we cannot see the distinguishable target return. And figure 7 is representation of same in Speed-Time domain. Figure 8 indicates the STAP Beam forming mechanism. Here radar is forming Null in direction of jammer. And following figure for received waveform after STAP technique.

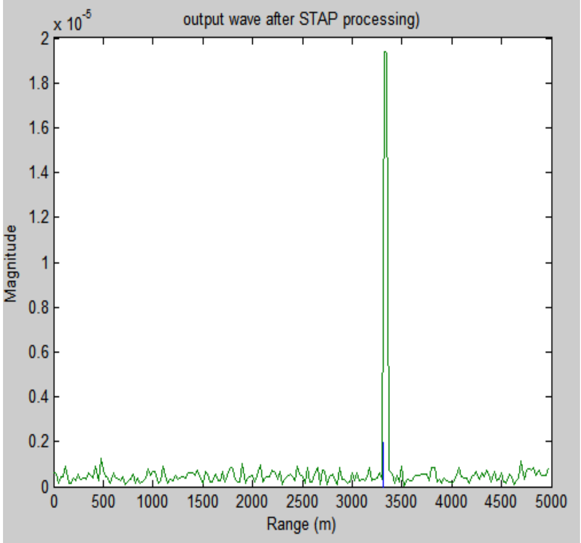

Figure 9: Received Waveform after STAP

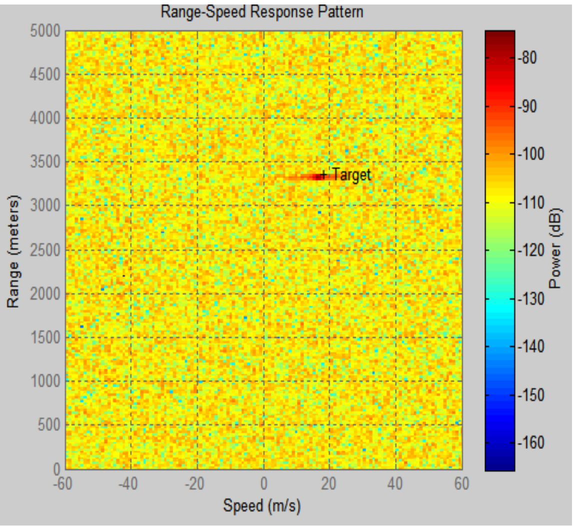

Figure 10: Speed Range response after STAP

3.2 Deception jamming:

Table 3: Radar specification for matlab simulation

Pulse width	1	µs
PRF	10	Khz
Carrier freq.	10	Ghz
Sampling freq.	1	Mhz
Tx. Power	600	KW
Tx.ant. gain	20	-
SNR (req)	11	-

Table 4: configuration of radar, jammer and target

	Position	*Range km*	*Relative angle*	*Relative speed*
Radar	(0,0,0)	-	-	-
Target 1	(1500,3500,200)	3.8 Km	(66,3)	6m/s
Target 2	(3500,5500,200)	6.5	(57,2)	30m/s
Target 3	(7000,7000,500)	9.9	(45,3)	17m/s
Jammer	(6000,4000,100)	7.2	(33,0)	33m/s

Jammer power = 1Kw
Deception type – Range

Here we consider three target at three different location and different travelling speed.

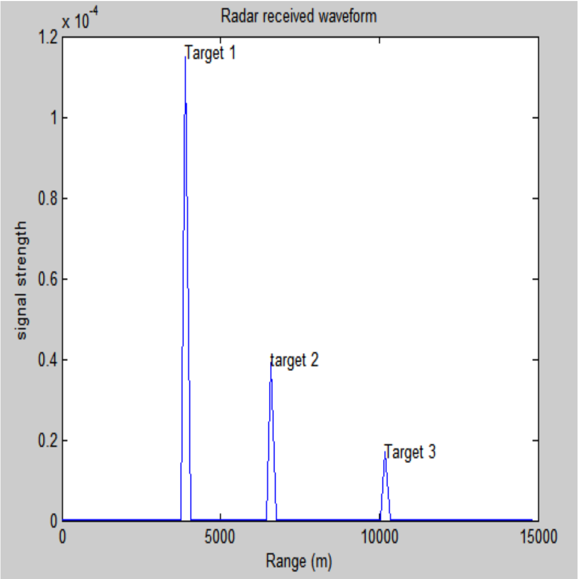

Figure 11: Received waveform under normal radar operation

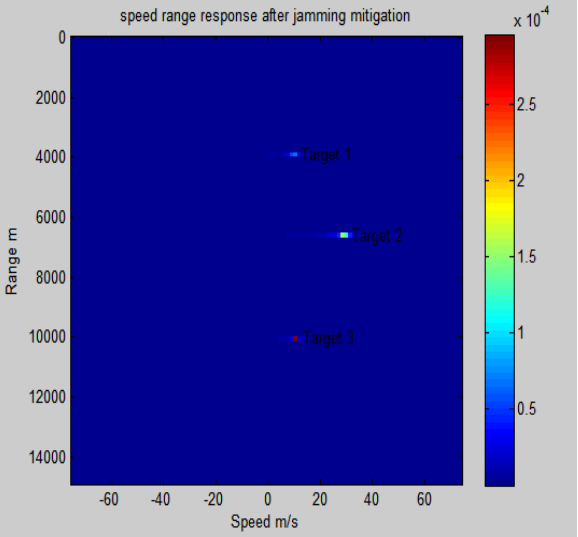

Figure 12: Speed Range response at normal radar radar operation.

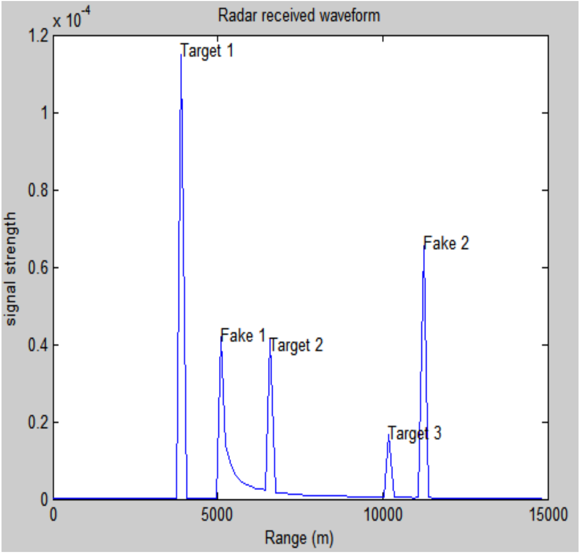

Figure13: Waveform received under deception jamming

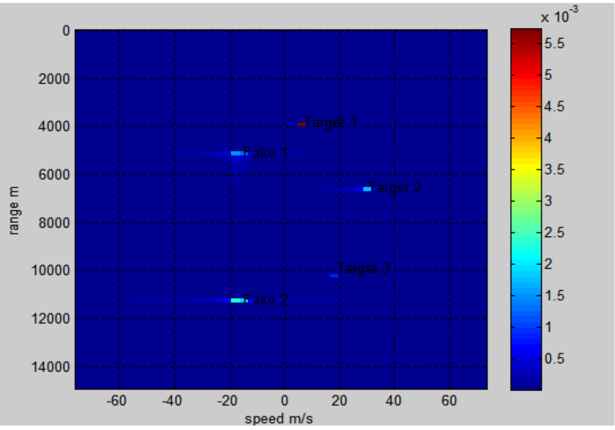

Figure 14: Speed Range response under deception jamming.

During deception jamming we are injecting the radar screen with two extra non existing fake target. The above both figure is evident for that.

Mitigation of deception jamming: power stagger pulse with differential receiver

Radar transmitting power P1=0.6Mw
p2=3Mw.

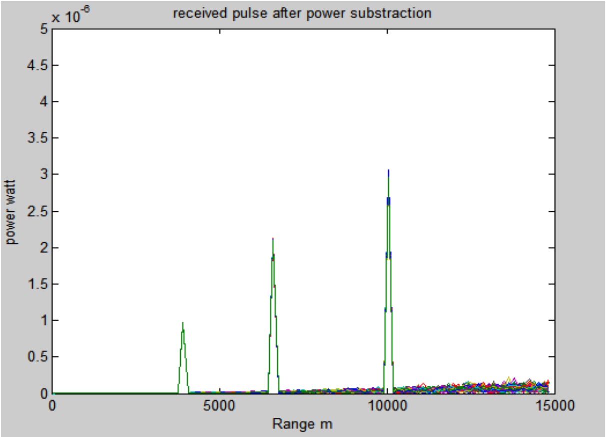

Figure 15: Waveform received after deception jamming mitigation

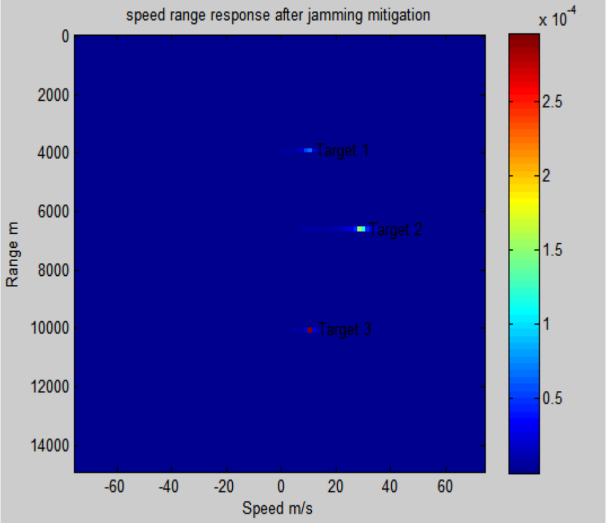

Figure 16: Speed Range response after jamming mitigation.

Figure above indicates received waveform by radar after jamming mitigation from which we can clearly see real target.

3.3 Inverse gain jamming:

Table 5: Radar specification for simulation.

Pulse width	0.33	µs
PRF	30	Khz
Carrier freq.	10	Ghz
Sampling freq.	6	Mhz
Tx. Power	5.2	KW
Tx.ant. gain	20	-
SNR (req)	5	-

Table 6: Configuration of jammer, Radar and target

	Position	*Range m*	*Relative angle*	*Relative speed m/s*
Radar	*(0,0,0)*	-	-	-
Targe	*(3000,2000,100)*	*3606*	*(33,0)*	*55*

jammer, power=500watt

here we consider a jammer and target as a single platform. And we deployed inverse gain radar jamming technique so that the radar cannot see target (jammer). Figure below show radar scan display between +90 to -90 azimuth angle. First displays for normal radar operation. The red dot indicates that target is situated at azimuth angle of 33 degree.

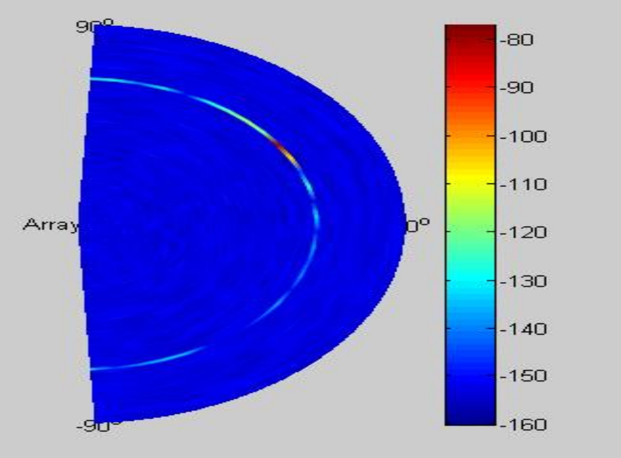

Figure 17: Radar scan display at normal condition

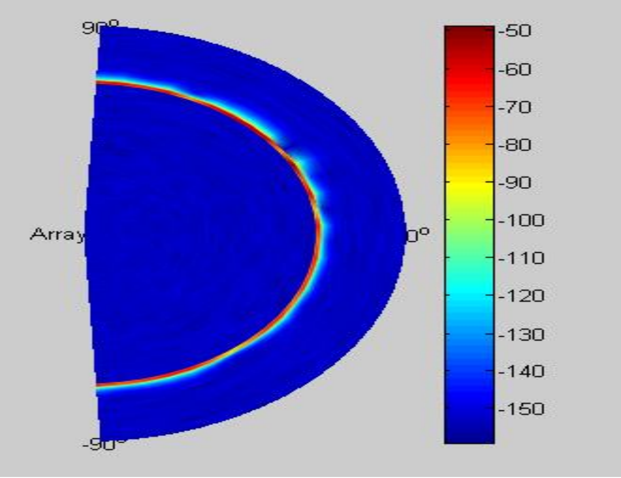

Figure 18: Radar scan display under IGJ jamming.

Here we can see a just ring instead of a single dot. Hence radar is said to be jam. and we cannot predict the target bearing at this condition.

Mitigation of IGJ: Power stagger pulse with differential receiver.

Radar transmitting power P1=5.2Kw,P2=0.52Mw

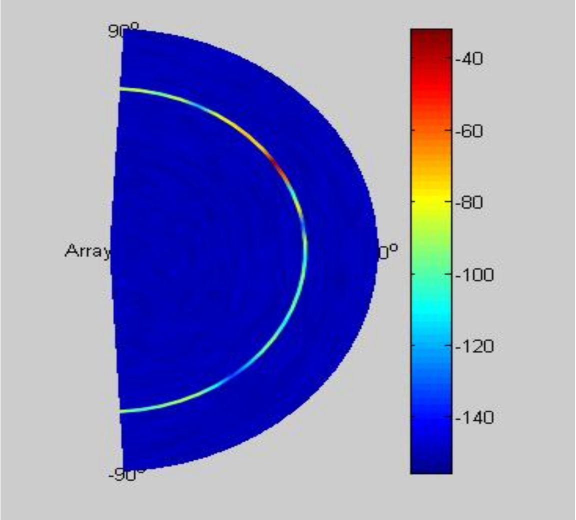

Figure 19: Radar scan display after jamming mitigation tech.

The above figure shows radar scan display after jamming mitigation technique is deployed. Here again we can see a clear target.

4. Conclusion

Basically this paper present two radar jamming techniques along with their mitigation technique. Here barrage and deception jamming technique are considered for surveillance radar. Beside that STAP and Power stagger pulse with differential receiver are used for mitigation purposes. Actually barrage jamming is more fruitful for low radar-jammer and high radar-target separation. Where-as deception jamming can be used for long distance jamming because back at radar receiver these jamming signals also get amplified as radar echo.

For deception jamming, the jammer should have the adequate knowledge of radar signal characteristics in order to synthesize offset jamming radar signal. This requires complex jamming module. Where-as for barrage jamming just knowledge of radar frequency is sufficient to create the jamming signal. In case of STAP radar receiver, if jammer and target are in same direction then target detection is voided. This is the main drawback of this technique. But also by the use of two radar receiver separated by enough distance can over-come this problem.

References

[1] Bassem R. Mahafza, Atef Z. Elsherbeni, 2013. Matlab Simulations For Radar Systems Design. pp(1-65)

[2] Janice Onanian Mcmahon., 1955. Space-Time Adaptive Processing On The Mesh Synchronous Processor. MCMAHON P(2-3).

[3] Fabian D. Lapierre,1 Jacques G. Verly,2 Braham Himed,3 Richard Klemm,4 Andmarc Lesturgie. 2006 Radar Space-Time Adaptive processing/Hindawi Publishing Corporation EURASIP Journal on Applied Signal Processing Volume, Article ID 93805, Pages 1–4 DOI 10.1155/ASP/2006/93805

[4] Wang Lu-Lu, Wang Hong-Qiang,Cheng Yong-Qiang, Qin Yu-Liang.2013, A Novel SINR And Mutual Information Based Radar Jamming Technique, Central South University Press and Springer-Verlag Berlin Heidelberg pp 1-6

[5] Edwin K. Stodola, Neptune, 1944, Assignor To The United States Of America As Represented By The Secretary Of War . Radar Receiver Automatic Gain Control Circuit Application, Serial No. 546,7263 Claims. (01. 250-20).

[6] Xiao Tian. 2012 Radar Deceptive Jamming Detection Based On Goodness-Of-Fit Testing Journal of Information & Computational Science 9: 13 3839–3847.

[7] Ch. Anoosha, Ch. Kusmakumari, M. Nirmala, Detection and Cancellation of Jamming Signal Noise Using Digital Filters for Radar Applications, International Journal of Electronics Communication and Computer Engineering, Volume 4, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

[8] Rajendra Prasad P, B. Abdul Rahim, 2012, Fast Self Switching type Frequency Agile RADAR Processing unit Implemented on Xilinx, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-1, Issue-2.

[9] Pula Sree Vishnu,2014, implementation of model radar target direction identifier, International Journal of Engineering & Science Research, IJESR/ Vol-4/Issue-3.

[10] Takayuki Inaba, 2007, Interference Suppression in FMICW Radar with Staggered Pulse Repetition Interval, Electronics and Communications in Japan, Part 1, Vol. 90, No. 12, Translated from Denshi Joho Tsushin Gakkai Ronbunshi, Vol. J88-B, No. 12, December 2005, pp. 2358–2371.

[11] Jonathan Schuerger, Dmitriy Garmatyuk,2008 Deception Jamming Modeling In Radar Sensor Networks, 978-1-4244-2677-5/08/$25.00 © IEEE.

[12] Adrian Graham, Communications, 2011 Radar and Electronic Warfare, first edition .pp(130-142)