

ELEKTRONİK HARP TEKNİKLERİ

VEYSEL DİNÇ

YÜKSEK LİSANS TEZİ

ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ŞUBAT 2010

ANKARA

Veysel DİNÇ tarafından hazırlanan “Elektronik Harp Teknikleri” adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Prof.Dr. Müzeyyen SARITAŞ

Tez Danışmanı, Elektrik-Elektronik Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği / oy çokluğu ile Elektrik Elektronik Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Prof.Dr. Nihal Fatma GÜLER

Telekomunikasyon Eğitimi Anabilim Dalı , Gazi Üniversitesi

Prof.Dr. Müzeyyen SARITAŞ

Elektrik-Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Yrd.Doç.Dr. T. Selcen NAVRUZ

Elektrik-Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Tarih : 18/02/2010

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof. Dr. Bilal TOKLU

Fen Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Veysel DİNÇ

ELEKTRONİK HARP TEKNİKLERİ**(Yüksek Lisans Tezi)****Veysel DİNÇ****GAZİ ÜNİVERSİTESİ****FEN BİLİMLERİ ENSTİTÜSÜ****Şubat 2010****ÖZET**

Elektronik harp, ülkeler arasında, sahip olunan teknoloji ve elde edinilen istihbarat bilgisine göre sürdürülen elektromanyetik spektrumun kontrolünü ele geçirme savaşıdır. 1905 Rus Japon savaşında telsiz sinyallerin karıştırılmasıyla başlayan ve ikinci dünya savaşı sırasında önemi kavranan elektronik harp teknolojisi, günümüzde de savunma teknolojilerinde ülkelerin birbirleriyle yarıştıkları bir alan olmaya devam etmektedir. Ülkeler yeni bir teknik geliştirmek için sürekli olarak yeni teknolojiler araştırmakta ve bu savaş tarihler boyunca sürüp gitmektedir.

Elektronik Harp faaliyetleri RF sinyaller ile başlamasına rağmen, teknolojik gelişmeler, daha üst bandlar olan IR ve UV bandlarının da kullanılmasına ve bu bandlarda elektronik harp sistemlerinin üretilmesine imkan sağlamaktadır.

Bu çalışmada, öncelikle Elektronik Harp terminolojisi ele alınmış, hava platformlarında kullanılan elektronik harp sistemleri üzerinde durulmuştur. Daha sonra RF karıştırma teknikleri ve çeşitleri açıklandıktan sonra, günümüzde karıştırma tekniklerinde kullanılan Digital Radio Frequency Memory (DRFM) detaylı olarak incelenmiştir. Bu kapsamda, MatLab Simulink programı kullanılarak DRFM modellenmiştir. Bu DRFM modeli ile karıştırma

tekniklerinden; çoklu sahte hedef yaratma (Multiple False Target Generation), Range Gate Pull Off (RGPO) ve Velocity Gate Pull Off (VGPO) olmak üzere 3 farklı karıştırma tekniği uygulanmıştır. Çoklu sahte hedef yaratma uygulamasında, izleme modundaki radara, bir uçak birbirinden farklı mesafelerde 5 adet uçak varmış gibi gösterilmiştir. RGPO uygulamasında, radarın mesafe kapısı çalınarak, radara doğru yaklaşan bir uçağın uzaklaşıyormuş gibi algılanması sağlanmıştır. VGPO uygulamasında ise, uçak olduğundan daha hızlı hedefe yaklaşıyormuş izlenimi verdirilmiştir.

DRFM modeli kullanılarak; modelde kullanılan bloklara ait parametrelerle, ilgilenilen tehdide ait parametreler aynı olacak şekilde seçilerek, hangi karıştırma tekniğinin hangi tehdide karşı etkili olacağı araştırılabilir. Ayrıca bu modelden elde edilen çıkış sinyallerinden, örnekleme ve dilimleme sırasında oluşan istenmeyen gürültü ve sahte sinyaller incelenerek, DRFM ile üretilmiş aldatma sinyalinin gerçek sinyalden ayırt edilebilmesi konusunda çalışma yapılabilir.

Bilim Kodu : 905.1.034

Anahtar Kelimeler :Elektronik Harp Teknikleri

Sayfa Adedi : 64

Tez Yöneticisi : Prof.Dr. Müzeyyen SARITAŞ

ELECTRONIC WARFARE TECHNIQUES**(Ms. Sc. Thesis)****Veysel DİNÇ****GAZİ UNIVERSITY****INSTITUTE OF SCIENCE AND TECHNOLOGY****February 2010****ABSTRACT**

Electronic Warfare (EW) is the war among countries of taking control of electromagnetic spectrum based on technology and intelligence information obtained. EW technology started with jamming radio signals in Russian-Japanese war in 1905 and its importance was understood during the second world war, and it continues to be a field where countries compete today. Countries do research for new technologies continuously in order to develop new techniques and this war lasts all history long.

Although, EW activities started with RF signals, technological developments make it possible for EW to be used and EW systems to be produced in IR and UV bands which are upper bands

In this study, it is dealt first with EW terminology and then with EW systems used in air platforms. Later, RF jamming techniques and types are explained, DRFM used in jamming techniques in our day are analyzed in detail. In this respect, DRFM is modeled using MatLab Simulink Program. With this DRFM model, three different jamming techniques, Multiple False Target Generation (MFTG), Range Gate Pull Off (RGPO) and Velocity Gate Pull Off (VGPO) are used. In the application of MFTG, a plane is shown as if it were 5 planes at

different distances from one another to a radar in surveillance mode. In the RGPO application, stealing range gate of the radar, the radar is made to believe that a plane approaching the radar is getting away. As for the application of VGPO, the impression is given that the plane is travelling faster than its real speed.

Using DRFM model, it may be researched which jamming technique is effective against which threat, choosing the parameters of blocks used in the model the same as the parameters of the threat in question. Furthermore, one may also study the subject of differentiating the deceiving signal produced by DRFM from the real signal through studying unwanted noise and spurious signals coming out during sampling and quantization from the output signals gained in this model.

Science Code	: 905.1.034
Key Words	:Electronic Warfare Techniques
Page Number	: 64
Adviser	: Prof.Dr. Müzeyyen SARITAŞ

TEŞEKKÜR

Öncelikle, tez çalışmam boyunca, tezi bitirmem konusunda beni cesaretlendirerek çalışmaya sevk eden, değerli tavsiyelerde bulunan, desteklerini hiç esirgemeyen ve sabırla beni yönlendiren tez danışmanım Prof. Dr. Müzeyyen SARITAŞ'a teşekkürlerimi sunmaktan kıvanç duyarım.

Elektronik Harp konusunda gerekli eğitimleri almama ve uygulamalı olarak bu alanda çalışmama imkan sağlayan Hava Kuvvetleri Komutanlığı'na şükranlarımı sunarım.

Gösterdikleri destek ve sabırdan dolayı eşim Kadriye DİNÇ'e ve çocuklarım Bahadır Sarper, Gizem ve İrem'e teşekkürü bir borç bilirim.

İÇİNDEKİLER

	Sayfa
ÖZET.....	iv
ABSTRACT.....	vi
TEŞEKKÜR.....	viii
İÇİNDEKİLER.....	ix
ŞEKİLLERİN LİSTESİ.....	xii
SİMGELER VE KISALTMALAR.....	xiv
1. GİRİŞ.....	1
2. ELEKTRONİK HARP.....	3
2.1 Elektronik Harbin Tarihçesi.....	3
2.1.1. 1905 Rus-Japon Savaşı.....	3
2.1.2. 2 nci Dünya Savaşı.....	3
2.1.3. Soğuk Savaş Dönemi.....	4
2.1.4. Vietnam Savaşı.....	5
2.1.5. Arap – İsrail Savaşları.....	5
2.1.6. 1980’li Yıllar.....	6
2.1.7. Körfez Savaşı.....	6
2.2. Elektronik Harbin Tanımı.....	7
2.2.1. Elektronik harp destek sistemleri (Electronic Support – ES)...	8
2.2.2. Elektronik taarruz (Electronic Attack – EA).....	10

	Sayfa
2.2.3. Elektronik korunma (Electronic Protection – EP).....	12
3. ELEKTRONİK HARPTE TEKNOLOJİ KULLANIMLARI.....	14
3.1. Elektronik Harpte IR/UV/Lazer Teknolojisi Kullanımı.....	14
3.1.1. IR ve UV Tabanlı Füze İkaz Sistemleri.....	14
3.1.2. Lazer İkaz Alıcıları (Laser Warning Receiver-LWR).....	15
3.1.3. IR Karıştırıcılar.....	16
3.2. Elektronik Harpte RF Teknolojisi Kullanımı.....	18
3.2.1. Radar İkaz Alıcıları.....	18
3.2.2 RF Karıştırıcılar.....	19
3.2.3. Görünmezlik (Stealth) Teknolojisi.....	27
3.3. Karıştırma Yöntemlerinin Harekatta Kullanım Konseptleri.....	28
3.3.1. Korunma karıştırması (Self Screening Jamming – SSJ).....	28
3.3.2. Refakatte karıştırma (Escort Jamming – EJ).....	29
3.3.3. Uzaktan karıştırma (StandfOff Jamming - SOJ).....	30
3.4. Hava Platformlarında Tümlşik EW Suite Sistemleri.....	30
4. DRFM (DIGITAL RADIO FREQUENCY MEMORY) TEKNOLOJİSİ.....	33
4.1. DRFM'in Tanımı ve Kapsamı.....	33
4.2. Günümüzde Kullanılmakta Olan DRFM'lere İlişkin Tanımlar.....	38
4.2.1. Anlık band genişliği (Instantaneous Bandwidth- IBW).....	38
4.2.2. Frekans ayar aralığı.....	38
4.2.3. Lokal osilatör ihtiyacı.....	39

	Sayfa
4.2.4. DRFM duyarlılığı.....	39
4.2.5. Dinamik aralık.....	39
4.2.6. Örnekleme gereksinimi.....	40
4.2.7. Dilimleme gereksinimi.....	40
4.2.8. Depolama gereksinimi.....	40
4.3. DRFM Uygulamasında Simulink Programı Kullanımı	41
4.3.1. Sayısal faz odülasyonu (Phase Shift Keying-PSK).....	41
4.3.2 QPSK (Quadrature Phase Shift Keying).....	42
4.3.3. Raised cosine transmit filter.....	43
4.3.4. AWGN kanalı.....	44
4.4. DRFM Modellemesi ve Aldatma Karıştırması.....	44
4.4.1. Temsili radar sinyalinin oluşturulması.....	46
4.4.2. DRFM girişindeki sinyalin tekrar elde edilmesi.....	47
4.4.3. DRFM girişindeki sinyalin kaydedilmesi.....	48
4.4.4. Farklı mesafelerde sahte çoklu hedef yaratılması.....	49
4.4.5. Hız kapısı çalınması tekniği.....	51
4.4.6. Mesafe kapısı çalınması tekniği.....	57
5. SONUÇ VE ÖNERİLER.....	60
KAYNAKLAR.....	62
ÖZGEÇMİŞ.....	64

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1 Lazer Silahı.....	11
Şekil 2.2 HARM Füzesi.....	12
Şekil 3.1 Füze İkaz Sistemleri.....	15
Şekil 3.2 Lazer Podu.....	16
Şekil 3.3. IR Karıştırıcı Sistem.....	17
Şekil 3.4. DIRCM Sistemi.....	17
Şekil 3.5 Flare Atışı.....	18
Şekil 3.6 RGPO Tekniği.....	22
Şekil 3.7 VGPO Tekniği.....	23
Şekil 3.8 Açık Aldatması.....	24
Şekil 3.9 Chaff Kullanımı.....	25
Şekil 3.10 Chaff/Flare Atma Sistemi.....	25
Şekil 3.11 Sahte Hedef.....	27
Şekil 3.12 Görünürlüğü Azaltılmış Uçaklar.....	27
Şekil 3.13 Kendini Koruyan Uçak.....	29
Şekil 3.14 Refakatte Karıştırma.....	29
Şekil 3.15 Uzaktan Karıştırma.....	30
Şekil 3.16 Tümüleşik EW Suite Sistemi.....	32
Şekil 4.1 DRFM Blok eması.....	34

Şekil	Sayfa
Şekil 4.2 DRFM'in Lineer RGS'si için zaman gecikme fonksiyonu.....	36
Şekil 4.3 DRFM Simulink Modeli.....	45
Şekil 4.4 Temsili Radar Sinyali.....	46
Şekil 4.5 DRFM Girişine Gelen Sinyal.....	47
Şekil 4.6 Direkt Yol Çıkış Sinyali.....	48
Şekil 4.7 DRFM'de Kaydedilen Sinyal.....	49
Şekil 4.8 Sahte Hedef Yaratma Simulink Modeli.....	50
Şekil 4.9 Sahte Hedef Sinyalleri.....	51
Şekil 4.10 VGS Simulink Modeli.....	52
Şekil 4.11 CPS Girişindeki Sinyal.....	53
Şekil 4.12 Faz Farkı Yaratılmadan Önceki Sinyal.....	53
Şekil 4.13 VGS-1 Sinyali.....	54
Şekil 4.14 CPD Çıkışı-1 Sinyali.....	55
Şekil 4.15 RGS Simulink Modeli.....	57
Şekil 4.16 Lineer RGS Sinyali.....	58
Şekil 4.17 RGS Fark Gecikme Sinyali.....	58

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılan bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
AGC	Automatic Gain Control
AOA	Angle Of Arrival
ARM	Anti Radiation Missile
CW	Continous Wave
DIRCM	Directed IR Countermeasure
DRFM	Digital Radio Frequency Memory
EA	Electronic Attack
ECCM	Electronic Counter Countermeasure
ECM	Electronic Countermeasure
EH	Elektronik Harp
EJ	Escort Jamming
ELINT	Electronic Intelligence
EM	Elektromanyaetik Spekturum
EP	Electronic Protection
ESM	Electronic Support Measure
EW	Electronic Warfare
IBW	Instantenous Band Width
IRCM	IR Countermeasure
LWR	Laser Warning Receiver
MWS	Missile Warning System
PRF	Darbe Repetition Interval
PRI	Darbe Repetition Interval
PSK	Phase Shift Keying
PW	Darbe Width

RGS	Range Gate Stealer
RGPO	Range Gate Pull Off
RIAS	Radar İkaz Alıcı Sistem
RWR	Radar Warning Receiver
QPSK	Quadrature Phase Shift Keying
SIGINT	Signal Intelligence
SNR	Signal to Noise Ratio
SOJ	Stand-off Jammer
SSJ	Self Screening Jamming
VCO	Voltage Control Oscillator
VGS	Velocity Gate Stealer
VGPO	Velocity Gate Pull Off
TOA	Time Of Arrival

1. GİRİŞ

Elektronik Harp (EH), teknolojinin imkanlarını en iyi biçimde kullanarak, Elektromanyetik Spektruma hâkim olmak ya da başkalarının aleyhte kullanamayacağı biçimde EM Spektrumu kontrol altında tutabilmek için verilen teknoloji savaşıdır. Elektronik Harpte başarı için sahip olunması gerekli mutlak 2 unsur vardır. Bunlardan birincisi; başkalarının henüz fark etmediği teknolojileri keşfederek, bu yeni teknolojiyi kullanan sistem geliştirerek kullanabilmek, ikincisi ise çok iyi bir istihbarat çalışması yapabilmektir. Hem iyi istihbarat yapabilmek ve hem de benzeri bulunmayan sistemlere sahip olmak için ileri teknoloji kullanımı esastır. İleri teknolojisi bulunmayan bir ülke iyi istihbarat elde edemediği gibi, başka ülkelerin istihbaratlarına da karşı koyamaz. Eğer bu ülke başka bir kaynaktan istihbarat edinebilse bile, hedef ülkelerin elektronik taarruzuna karşı, karşı tedbir geliştiremeyeceğinden istihbarat bilgisi bir fayda sağlamayacaktır.

Genel olarak EH faaliyetleri;

1. Tehdit olarak görülen bölgede EM sinyalleri toplanması,
2. Bu sinyallerden hangilerinin tehdit silah sistemine ait olduklarının tespit edilmesi,
3. Tehdit silah sisteminin yerinin ve ayrıntılı teknik özelliklerinin belirlenmesi,
4. Elde edilen bu bilgilerin kullanılarak bu bölgeye yaklaşıldığında, daha önce tespit edilen bu tehdidin EM spektrumu doğru/etkin kullanamaması ya da hiç kullanamaması için gerekli tedbirlerin alınması esasına dayanır.

Elektronik harp faaliyetleri Kara, Deniz, Hava gücü unsurları için kullanılır, ya da müşterek bir taarruz için her üç unsurun birlikte yürütülür. Müşterek taarruzda bu unsurlar birlikte hareket etmek ve koordineli teknikler uygulamak zorundadırlar, aksi halde bu üç unsur birbirlerinin faaliyetlerini olumsuz olarak etkileyerek birbirlerine zarar verebilirler.

Elektronik Harp faaliyetleri düşman radar ve silah sistemlerinin tespit ve teşhisi ile başlar. Herhangi bir elektronik saldırıya karşı tedbir geliştirebilmek için önce o saldırıyı algılamak gerekmektedir. Buradan hareketle geliştirilen ilk EH sistemleri

Radar İkaz Alıcı Sistemler (RİAS) olmuştur. RİAS'lar geliştirildikten sonra, teşhis edilen hedefi etkisiz kılmak için karşı tedbirler geliştirilmeye çalışılmıştır. Düşman radarı tarafından tespit edilmeyi önlemek üzere, başlangıçta karşı tedbir olarak karıştırma teknikleri geliştirilmiştir. Karıştırma sinyallerinin radarlar tarafından ayırt edilmeye başlanması üzerine, karıştırma tekniğinden farklı olarak gelen radar sinyalini geciktirerek gönderme kabiliyetine sahip Frequency Memory Loop (FML) kullanılmaya başlanmıştır. Zaman geçtikçe radarlardaki teknolojik gelişmeler sayesinde FML'ler de artık yetersiz kalarak Digital Radio Frequency Memory (DRFM) teknolojisine geçiş yapılmıştır. Günümüzde DRFM teknolojisindeki gelişmeler hızla devam etmektedir.

EM spektruma tamamen hakim olmak isteyen gelişmiş ülkeler RF bandını kullanmakla yetinmeyip, daha üst bandları da kullanabilmek için çalışmalara yönelmişlerdir. Bu kapsamda ilk uygulamalar kızıl ötesi-IR bandında başlatılarak ısı güdümlü füzeler yapılmış, hemen ardından da bu füzeleri önceden algılamak üzere Füze İkaz Sistemleri ve IR karıştırma sistemleri geliştirilmiştir.

Unutulmamalıdır ki, kimse savaş ilan etmese ve bilinen sıcak bir cephe olmasa bile elektronik harp her an devam etmektedir. Ülkeler, devam eden bu savaşın neresinde olduklarını iyi değerlendirmeli ve gerekli önlemleri süratle almalıdırlar.

2. ELEKTRONİK HARP

Elektronik Harp (EH), teknolojinin imkanlarını en iyi biçimde kullanarak, Elektromanyetik Spektruma hâkim olmak ya da başkalarının aleyhte kullanamayacağı biçimde ElectroMagnetic Spektrumu kontrol altında tutabilmek için verilen teknoloji savaşıdır. Bu bölümde öncelikle EH'in tarihçesi verildikten sonra EH genel kavramları üzerinde durulmuştur.

2.1. Elektronik Harbin Tarihçesi

Elektronik Harbin öneminin anlaşılabilmesi ve bu alanda ileriye yönelik ilerlemelerin sağlanması için elektronik harbin tarihçesine yer verilmiştir.

2.1.1. 1905 Rus-Japon savaşı

Tarihte, telsiz sinyalleri karıştırma amaçlı olarak ilk kez bu savaşta kullanılmıştır. Japon keşif gemileri, Rus donanmasının muhaberesinden elde ettiği istihbarat bilgileri (Rus donanmasının savaş düzeni, operasyon planları v.b.) ile savaşın seyrini değiştirmişlerdir.

2.1.2 İkinci dünya savaşı

Bismarck gemisinin batırılması

İngiliz ticaret gemilerini engellemekle görevlendirilen Almanların Bismarck gemisinde, dünyanın bilinen ilk Radar İkaz Alıcısı olan ve 100-500 MHz. frekans bandında çalışan Metox cihazı kullanılmıştır.

Channel Dash uygulaması

Tarihte bilinen ilk Elektronik Taarruz (ET) uygulamasıdır. Mart 1941’de Almanlar Dover’e gelinceye kadar İngilizlerin Manş Denizi’ni kontrol eden radarlarını karıştırarak İngilizler tarafından mümkün olabildiğince o bölgeden yapılacak geçişin geç tespitini sağlamışlardır.

Müttefiklerin Almanya hava saldırısı

Müttefiklerin Almanya’ya yaptıkları hava taarruzlarının önemli bir yönü de tarihte ilk defa CHAFF kullanılmış olmasıdır. 24 Temmuz 1943 tarihinde bir Alman radar operatörü yeni bir hava taarruzu ile karşı karşıya kaldığını tespit ettikten kısa bir süre sonra ekranda çok sayıda uçağın geldiğini görür. Tabii olarak bu kadar çok uçağın bir anda ortaya çıkmasının mümkün olamayacağı için, radarının arızalandığını düşünür. Yapılan kontroller ile aslında radarın fonksiyonel biçimde çalıştığı ve ekrandaki bu karışıklığın nedeninin CHAFF kullanılmasından kaynaklandığı anlaşılır.

2.1.3. Soğuk savaş dönemi

Soğuk savaş döneminde kurulan gerek NATO ve gerekse Varşova Paktları, soğuk savaş döneminin en önemli silahı olan Elektronik Karıştırma faaliyetlerine yöneldiler. Önce Ruslar faaliyete geçti ve doğu bloğu ülkelerine yayın yapan Amerika’nın Sesi ve BBC radyo istasyonlarında karıştırma yaptılar. Ruslar, adı geçen radyo yayınlarını etkisiz kılabilmek için 800’ü kendi ülkelerinde 700’ü diğer ülkelerde olmak üzere 1500 civarında karıştırma istasyonu tesis ederek uygulamaya 1959 yılına kadar devam ettiler.

Yeni Rus radarları hakkında hiçbir şey bilmediğini fark eden Batı, 1949 yılından itibaren Ruslara karşı Elektronik İstihbarat (Electronic Intelligence-ELINT) faaliyetlerine başladı. Etkili bir ELINT faaliyeti için karşı tarafın yeteneklerinin tespiti gerektiğinden bu dönemde bloklar arasında karşılıklı olarak hava sahası

ihlallerinin arttığı gözlenmiştir. Soğuk Savaş döneminde ortaya çıkan diğer önemli Elektronik Harp (EH) / Sinyal İstihbaratı (Signal Intelligence-SIGINT) uygulamaları arasında; SIGINT Merkezlerinin kurulması yer almaktadır.

2.1.4. Vietnam savaşı

Amerikalılar Vietnam Savaşı esnasında hem Radar İkaz Alıcılarını daha geliştirdiler, hem de yayına doğru giden füzeleri (ARM - Anti Radiation Missile) uygulamaya koydular. F-4 uçaklarına hem Radar İkaz Alıcılarını hem de yayına giden füzeleri yerleştirerek onların tabiri ile Wild Weasel hareket tipini geliştirdiler. Ruslar Fansong radarının frekans bandını 3 GHz civarından 5 GHz civarına çıkardılar ve diğer bir teknik daha uyguladılar. Bu Wild Weasel görevinde, sadece F-4 uçakları değil B-52 uçakları da kullanılıyordu. 1972 yılına gelindiğinde Amerikalılar, EA-6B Uzaktan Karıştırma Elektronik Harp uçaklarını devreye soktular. Bu uçaklar çok şiddetli karıştırma yaparak Vietnam radarlarını köreltiyorlardı. Bu esnada ilk Bilgisayar Kontrollü Radar İkaz Alıcısının da kullanılmaya başlandığı bilinmektedir.

2.1.5. Arap – İsrail savaşları

1973 yılında Mısırlılar, Rusya'dan iki değişik füze sistemi daha almışlardı. Birisi SA-6 olarak bilinen SAM sistemi, diğeri de GUNDISH olarak bilinen radarlı uçaksavar sistemiydi. Bunların özelliklerini İsraililer bilmedikleri için Yom Kippur savaşının ilk günlerinde büyük kayıp verdiler. SA-6 sisteminin özelliği CW (Sürekli Dalga) aydınlatması yaparak füzeyi yönlendirmesiydi. O güne kadar radarlar, hep darbeli radar olarak karşılara çıkıyordu. Bu yüzden CW yayın yapan bir füze sistemine karşı tedbir uygulayacak bir teçhizat İsrail'lilerin ellerinde yoktu. GUNDISH Radarları ise 16 GHz civarında çalışıyordu. O güne kadar 12 GHz'in üstünde çalışan bir sisteme sahip olmayan İsraililer için bu şaşırtıcıydı. Çünkü ellerindeki teçhizat ile GUNDISH radarlarını tespit ve teşhis edemiyorlardı. Buna karşın, İsraililer her iki radara karşı da Chaff uygulamasına geçtiler ve hayret verici bir şekilde GUNDISH radarına karşı başarılı oldular. Chaff uygulaması aynı zamanda

hayli zor uçak manevralarıyla birleştirildi ve İsrail savaşın sonunda iyi sonuçlar elde etti.

2.1.6. 1980’li yıllar

Falkland savaşı

1980’lerin başına gelindiğinde Arjantin ile İngiltere arasında Falkland adaları üzerinde anlaşmazlık çıktı. Arjantinliler, ana kara Arjantine çok yakın olan adaları işgal ettiler. Falkland savaşı başladığı sırada İngilizler kuvvetlerini Arjantin’e gönderdiler ve burada HARRIER Uçaklarını kullandılar. Ancak Arjantinlilerin elinde de batı ülkelerinin geliştirdiği silahlar vardı. (Örneğin TPS-43 üç boyutlu radarlar, Roland Füze Sistemleri v.b. gibi). Bu sistemlere karşı İngilizler hızlandırılmış bir elektronik savunma amaçlı bir program yapmaya karar verdiler ve aşağıdaki 16 gün içinde 9 adet Kendini Koruma EH podunun geliştirilmesi, üretilmesi ve yerine gönderilmesi işlemini gerçekleştirdiler.

Bekaa vadisi savaşı

Bu savaş, Elektronik Harp ile koordineli olarak; Gerçek zamanda bilgi toplama, Bilgiyi yerine ulaştırma, Derhal değerlendirme ve Bilginin hedefe saldırı unsurları tarafından peş peşe kullanıldığı ilk savaş olmasından dolayı ilginç sayılmaktadır.

Ayrıca İsrail bu savaşta EH amaçlı özel İHA (İnsansız Hava Aracı)’ları kullandı. İHA’lar TV kamerası, lazer işaretleyici (laser designator) ve uçak ekosu yaratacak yansıtıcılar ile donatılmışlardı.

2.1.7. Körfez savaşı

Elektronik Harbin en son ve en etkili örneği ise Körfez Savaşı sırasında görülmüştür. Bu savaş modern hava savaşının yürütülmesinde EH’in önemini gözler önüne sermiş ve EH alanında modern batı doktrinine güzel bir çalışma konusu teşkil etmiştir. Müttefiklerin uyguladığı EH hareketıyla; Irak entegre hava savunma sistemi

çökertilerek entegre yapı bozulmuş, Müteakiben bölge ve nokta savunma sistemleri sürekli High speed Anti Radiation Missile (HARM) baskısı altında sistematik olarak devre dışı bırakılmıştır.

Körfez Harekatında EH Görevleri : Şimdi de paket kolda yer alan EH görevlerinin Körfez harekatında icra ediliş usulüne bir göz atalım. EH perspektifinden bakıldığında, Körfez Harekatı iki safhada gerçekleşmiştir.

Birinci safha

Bu safhada Elektronik Harekat Kapsamında ; EF-111 Uçakları, düşmanın radar görüntülerini etkili bir şekilde köreltmek için muharebe bölgesinde elektronik karıştırma yapmakla görevlendirilmiştir. EC-130 ve RC-135 uçakları, Irak'tan elde ettikleri elektronik faaliyet bilgilerini taarruz uçaklarına aktarmışlar, böylece bu safhada yoğun EH uygulamaları yapılmıştır.

İkinci safha

Taarruz uçakları hedeflerine yaklaşırken, Destek Uçuş Grubundan gerekli bilgileri almışlardır. Taarruz paketlerinin içinde yer alan, Wild Weasel uçakları (F-4G, F-16), Irak SAM'larını ve radarlarını etkisiz hale getirmişlerdir. Böylece taarruz paketinin emniyeti sağlanmış ve görevin etkinliği artırılmıştır. Örnek olarak bir Paket Kol incelendiğinde, 24 bombardıman (Taarruz) uçağı için 10 uçağın Elektronik Harekat görevlerini icra ettiği görülmektedir. Bu durum taarruz kollarının bekası ve etkinliği için Elektronik Harekatın ne kadar önemli olduğunu göstermektedir.

2.2. Elektronik Harbin Tanımı

EH, teknolojinin imkanlarını en iyi biçimde kullanarak, Elektromanyetik Spektruma hâkim olmak ya da başkalarının aleyhte kullanamayacağı biçimde EM Spektrumu kontrol altında tutabilmek için verilen teknoloji savaşıdır. Genel olarak EH faaliyetleri; tehdit olarak görülen bölgede EM sinyalleri toplanması, bu sinyallerden

hangilerinin tehdit silah sistemine ait olduklarının tespit edilmesi, daha sonra tehdit silah sisteminin yerinin ve ayrıntılı teknik özelliklerinin belirlenmesi, elde edilen bu bilgilerin kullanılarak bu bölgeye yaklaşıldığında, daha önce tespit edilen bu tehdidin EM spektrumu doğru/etkin kullanamaması ya da hiç kullanamaması için gerekli tedbirlerin alınması esasına dayanmaktadır.

EH Sistemlerini; EH destek sistemleri, EH taaruz sistemleri ve EH korunma sistemleri olmak üzere faaliyetlerini 3 ana bölümde inceleyebiliriz.

2.2.1. Elektronik harp destek sistemleri (Electronic Support – ES)

Düşman kuvvetlerinin elindeki savunma ve saldırı sistemlerinin tespit edilmesine yönelik faaliyetlerin tümüdür. Bu faaliyetler düşman yayınlarının algılanmaları, tanımlanmaları, analiz edilmeleri ve yerlerinin tespit edilmeleri için yürütülür. RF Sinyal ile çalışan bir sisteme ait sinyal ancak bir parametre setiyle tanımlanabilir. ES Sisteminde Kullanılan Parametrelerden bazıları; taşıyıcı frekansı, darbe genliği (Pulse Amplitude-PA), darbe genişliği (Pulse Width-PW), geliş zamanı (Time Of Arrival-TOA), yaklaşma açısı (Angle/Direction Of Arrival-AOA), polarizasyondur. Elektronik Harp Destek Sistemlerini 2 ana kategoriye ayırabiliriz. EH Destek sistemlerini, istihbarat ve ikaz sistemleri olmak üzere ikiye ayırabiliriz.

Elektronik istihbarat sistemleri (Electronic Intelligent - ELINT)

Bu sistemler, düşman bölgesine taarruz etmeden önce o bölgede bulunabilecek savunma ve saldırı sistemlerinin önceden tespit edilerek, bu sistemlere ait bilgi toplamaya yönelik olarak yapılmışlardır. RWR Sistemlerine göre boyutları büyüktür ve daha fazla sayıda sinyal parametresi ölçülür ve daha yüksek doğrulukta açı tespiti yapılabilir. Ayrıca bu tür sistemler RWR Sistemlerine göre çok daha uzak mesafelerden hedefi algılama kabiliyetine sahip çok daha duyarlı sistemlerdir. Böylece düşman hattına girmeden düşman hattının gerisinden elektronik sinyal istihbaratı yapılabilir. Bu sistemlerle elde edilen bilgiler, RWR sistemlerinin programlanmasında kullanılır.

İkaz sistemleri

Genellikle helikopter ve uçaklarda kendini koruma kabiliyeti kazandıran bu sistemlerin, radar ikaz alıcı, füze ikaz sistemi ve lazer ikaz alıcıları olmak üzere üç çeşidi vardır.

Radar İkaz Alıcı (Radar Warning Receiver-RWR)

Bu sistemler, tehdit arama, kilitleme radarları ile havadan havaya, yerden havaya atılan füze sistemleri ve uçaksavar mermi türü sistemlerin varlığını tespit ederek tehdidin ölümcül mesafesi içerisine girmeden önce tehdidi pilota ikaz etmektedir. RWR Sistemleri genel olarak tehdit kütüphanesine sahiptirler. Tehdit kütüphanesine operasyona gidilecek bölgede bulunması muhtemel tehditlere ait parametreler girilir. Bunun nedeni eğer operasyonsal bölgede RWR Sistemi ortamdaki tüm tehdit sinyallerini analiz etmeye kalksaydı, her sinyalin işlenmesi için ne yeterli zaman ne de bir jet uçağına sığacak büyüklükte bir sistem yapılabilirdi. Bu nedenle RWR Sistemine ait yazılım, yalnızca hedef bölgede tehdit olarak belirlenmiş sinyalleri arar. Algılanan tehdit sinyal parametreleri (Çalışma frekansı (RF), darbe tekrarlama frekansı (PRI), darbe genişliği (PW), darbe genliği, tarama periyodu, darbe tekrarlama frekansı (PRF), RF değiştirme özelliği (RF Hoping) gibi özellikler) analiz edilerek, bu sinyalin gerçekten de varlığı önceden tespit edilmiş tehdit sinyali mi olduğuna, tehdit kütüphanesindeki parametrelerle kıyaslama yapılarak karar verir. Tehdidin yeri DF yöntemiyle tespit edilerek, RWR ekranı vasıtasıyla, tehdidin ismi ve yeri pilota ikaz edilir. Operasyonel ortamda birden çok tehdit olması durumunda RWR Sistemi yazılımında belirtilmiş tarafından tehdit önceliklendirmesine göre tarama yapılır. Tehdit önceliklendirmesi belirlenirken tehditlerin öldürme güçleri esas alınır.

Füze İkaz Sistemi (Missile Warning System – MWS)

Bu sistemler havadan havaya veya yerden havaya atılan füze sistemlerinin attıkları füzeleri ateşleme anında yaydıkları IR ve UV ışınlarını üzerlerindeki sensörler ile algılayarak pilota ikaz verir. Genellikle, hava platformlarında ön ve arkada sağ ve sol olmak üzere sensörler yerleştirilmiştir. MWS ekranı üzerinde belirtilen dört yönden hangisinden füze tehditi algılanmış ise o yönden füzenin pilota doğru geldiği gösterilir. Bazı MWS’lerde gelen füzenin yönüne göre kaçılması gerekli yönde gösterilir. Genellikle MWS’ler chaff/flare atma sistemi ile koordineli çalışır. Füzenin geliş yönüne göre, tehdite karşı chaff/flare atışı için MWS’ten atış komutu üretilir.

Lazer İkaz Alıcıları (Laser Warning Receiver)

Bu sistemlerde, uçak üzerine, hedefin yerini belirtme amaçlı gönderilen bir lazer ışınının varlığını pilota ikaz eder. Genellikle lazer ikaz alıcıları DIRCM ile birlikte çalışırlar.

2.2.2. Elektronik taarruz (Electronic Attack – EA)

Elektronik taarruz, tehdit tarafından teşhis ve tespit edilmeyi engellemek maksatlı sinyal yaymak üzere yapılan faaliyetler olup, tahrip etmeyen ve tahribe dayalı olmak üzere iki çeşiti mevcuttur.

Tahrip etmeyen

Operasyon sahasına girerken düşman kuvvetleri tarafından teşhis ve tespit edilmeyi engellemek amacıyla, EM spektrumu kullanmayı engellemek yada kısıtlamak maksadıyla tahrip etkisi olmayan sinyal yayınlama ya da engelleyici çeşitli önlemlerin uygulanmasıdır. Genel olarak tahripsiz elektronik saldırı 3 ana bölümde incelenebilir. Bunlar Elektronik Aldatma, Elektronik Karıştırma ve düşman radarının görüşünü engelleyecek görünmezlik (Stealth) teknolojisi ya da Chaff/Flare/Decoy kullanılmasıdır. Bu konulardan üçüncü bölümde ayrıntılı olarak bahsedilecektir.

Tahribe dayalı

Düşmanın savunma sistemlerini tahrip etmek maksadıyla yayınlanan enerji olup, yönlendirilmiş enerji silahları ve anti radyasyon silahları olmak üzere iki çeşit uygulaması vardır.

Yönlendirilmiş Enerji Silahları

Çok yüksek seviyede enerji üretebilen ve bu enerjiyi bir yönlendirici ile hedefe göndererek, düşmanın personel ve teçhizatına zarar vermek suretiyle performansını düşüren veya imha/tahrip eden ET'nin tahrip maksatlı bir uygulamasıdır. Yönlendirilmiş enerji silahları türleri aşağıda sıralanmıştır.

1. Lazer silahları, yüksek enerji ve alçak enerji lazer silahları olmak üzere iki tipi mevcuttur. Şekil 2.1'de yönlendirilmiş bir enerji silahı olan Lazer silahı verilmiştir.



Şekil 2.1 Lazer Silahı

2. Yüksek güçlü mikrodalga silahları,
3. Tanecik ışıın silahları,
4. Akustik silahlar,
5. Plazma silahlarıdır.

Anti Radyasyon Silahları

Radar sistemlerini tahrip etmek veya RF ile çalışan sistemlerin belli bir süre kapatılmasını sağlamak, bu suretle düşmanın, hava savunma sistemlerini baskı altına almak için kullanılan tahrip güçlü silahlardır. Bu silahlardan en yaygın kullanımı olan HARM füzesidir. HARM, uçak hedefe yaklaşırken kendisini tehdit eden tehdide atılır. HARM nereden RF enerji yayılıyorsa oraya doğru yani RF kaynağına doğru yönelir ve çarparak kaynağı imha eder. Eğer hedef sistem HARM atıldığını algılayabilirse, korunma için RF yayını keser, bu sırada RF gönderemediği için hedefi takip edemeyeceğinden hedefe olan kilit kırılır. Bu sayede uçak kendisine füze atamayacak şekilde köreltilen tehdit sistemine taarruz etme imkanı bulur. Şekil 2.2’de HARM Füzesi resmi görülmektedir.



Şekil 2.2 HARM Füzesi

2.2.3. Elektronik korunma (Electronic Protection – EP)

Elektronik savunma amaçlı yürütülen faaliyetler Elektronik Korunma (Electronic Protection-EP) olarak adlandırılır. Bu faaliyetler genellikle sistemlerin elektronik taarruzlardan en az etkilenmesi için gerekli önlemlerin alınması şeklinde sürdürülür. Bu faaliyetlere, aşağıda bazı örnekler verilmiştir [15].

1. Hız artışı sınırlama
2. Uyumlu polarizasyonlu alıcı (adaptive receive polarization),

3. Aç ı uzan ım ın ı tahmin edici (angel extent estimator)
4. Band geniřlięi artırıcı (bandwidth expansion)
5. Aldatma frekansı tespitçisi (beat frequency detector)
6. Sabit yanlış-alarm hız ı kısıtlayıcı (censored CFAR)
7. Çapraz polarizasyon yok etme (cross-polization cancellation)
8. Doppler-menzil oran ı karřılařtırma (doppler-range rate comparison=
9. Frekans kaydırma (Frequency agility)
10. Karıřtırmaya yönelme (home-on-jame)
11. Darbe kenarlarını izleme (leading/trailing edge track)
12. Darband doppler gürültü algılayıcı (narrowband doppler noise dedector),
13. Dar darbe/darbe sıkıřtırma (narrow pulse/pulse compression),
14. Yandan izleme (off-boresight tracking)
15. Titreřimli Pulse Repetition Frequency (PRF Jitter)
16. Yan demet karartma (side lobe blanking)
17. Yan demet kesici (side lobe canceler)
18. Mevki ve zaman uyumlu iřleme(space time adaptive processing)
19. Hız korumalı kapılar (Velocity Guard Gates)
20. VGPO reset
21. Frekans atlama (Frequency Hoping)

3. ELEKTRONİK HARPTE TEKNOLOJİ KULLANIMLARI

EH elektromanyetik spektrumun ele geçirilme savaşı olması nedeniyle, EH faaliyetleri kapsamında alt bandlardan başlanarak, üst bandlara doğru giden bir kullanım söz konusudur. Bu kullanım o tarihlerde sahip olunan teknolojilerdeki sağlanan imkanlara bağlı olarak mümkün olmaktadır. EH uygulamalarına bakıldığında günümüzde kullanılan EH sistemlerinde kullanılan teknolojilerini IR/UV/Lazer teknolojisi ve RF teknolojisi olarak gruplamak mümkündür. Bu bölümde bahsedilen her iki teknoloji grubuna ait EH sistemleri ayrı ayrı ele alınacaktır.

3.1. Elektronik Harpte IR/UV/Lazer Teknolojisi Kullanımı

Elektromanyetik spekturumun IR ve daha üst bandları kullanılarak geliştirilen sistemler, IR ve UV Tabanlı Füze İkaz Sistemleri, lazer ikaz alıcıları ve IR karıştırıcı sistemler aşağıda açıklanmıştır.

3.1.1. IR ve UV tabanlı füze ikaz sistemleri (Missile Warning System – MWS)

RWR'lerin IR güdümlü füzeler gibi aktif sistemlere karşı etkisiz olmasından dolayı bu tip füzeleri tespit edebilmek ve gerekli önlemleri almak için MWS'ler geliştirilmiştir. MWS'leri, MLW sistemleri ve MAWS (Missile Approach Warning System) olarak iki gruba ayırabiliriz. MLW (Missile Launch Warning) sistemleri, füzenin IR ve UV imzasından yararlanarak füze motorunun egzostundan çıkan ateşten füzeleri tespit eder. IR füzelerin, IR ve UV imzaları, roket motorları durduktan sonra zayıflar. Füzeleri, fırlatma aşaması bittikten sonra da tespit edebilen MAWS, radar kullanarak, Doppler kayması ile tespit yapar. MLW sistemleri, füzenin yönünü hassas olarak belirleyebilirken; MAWS, füzenin mesafesini hassas olarak belirleyebilir. Ancak MAWS, yerleştirildikleri platformların RF görünürlüğünü artırır. Bu nedenle bu iki sistemin birlikte kullanılması daha yararlıdır. Önce MLW sistemi alıcıları kullanılarak, füze tehdidi tespit edilebilir ve hemen ardından MAWS devreye girebilir. İkaz sistemi, pilotu sesli ya da görsel olarak uyarabileceği gibi

doğrudan bir flare atma sistemine de bağlı olabilir. MWS, yancada 360° kapsama alanı sağlayacak ve platformun altına bakacak şekilde yerleştirilir. Şekil 3.1’de Füze İkaz Sistemine ait sensörler görülmektedir.



Şekil 3.1 Füze İkaz Sistemleri

3.1.2. Lazer ikaz alıcıları (Laser Warning Receiver-LWR)

LWR, taktik sahada platformlara doğrudan tehdit oluşturan lazer tabanlı sistemleri sezimleyebilmek için geliştirilmiştir. Lazer tabanlı sistemlerde hedef, bir lazer ışınımı ile işaretlenmektedir. İşaretleme ışınımını tespit edebilen LWR; işaretlemenin yönünü, PRF’sini ve PW’sini de tespit edebilir. Bu sayede LWR, ET sistemleri için de yönlendirici olabilir. Şekil 3.2’de uçaklarda kullanılan bir lazer podunun resmi verilmiştir.



Şekil 3.2 Lazer Podu

3.1.3. IR karıştırıcılar

IR dalga boyuna yönlenen silah sistemlerine karşı sahte hedef yaratarak, onları yaratan kaynağı ya da uçaktan yayılan IR yayılımı görmesini engelleyecek biçimde silah sistemini körelten sistemlerdir.

IRCM (Infared Counter Measure)

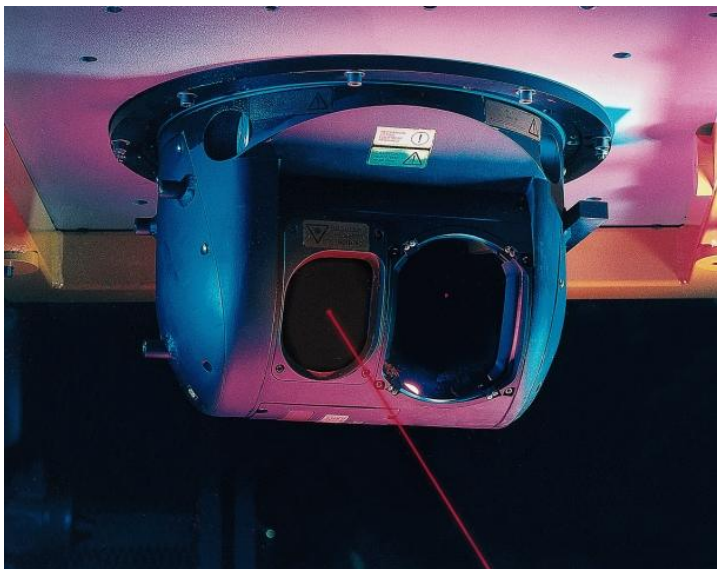
Tek başına bir IR kaynağı vasıtasıyla modüleli bir biçimde 360 derece etrafına IR enerji yayar. Uçağa yönelen füze uçak yerine bu sağa sola yayılan IR enerjiyi takip etmeye çalışır ve yörüngesinden saparak hedef bilgisini kaybeder. Şekil 3.3'de helikopterde kullanılan IR Karıştırıcı Sistem görülmektedir.



Şekil 3.3. IR Karıştırıcı Sistem

DIRCM (Directed Infared Counter Measure)

MWS Sistemi ile birlikte çalışır. MWS ile yeri tespit edilen IR tehdite laser sistemini yönlendirilerek, tehditin optiğine laser ışını göndermek suretiyle, IR sensörleri köreltir. Böylece tehdit uçağı algılayamaz hale gelir. Eğer tehdit sistemi IR güdümlü bir füze ise, füze uçağı ulaşmadan yörüngesini kaybeder. Şekil 3.4’de DIRCM Sistemi görülmektedir.



Şekil 3.4. DIRCM Sistemi

Flare kullanımı

Flare, Uçak ve gemilerden atılan, kızılötesi (IR) güdümlü füzelere karşı kullanılan sarf edilebilir malzemelerdir. Uçağın egzozundan çıkan ısıya yönelen füzeler, atıldığında yüksek ısı yayan flare'e yönelerek uçağın kilit kırmasına olanak sağlar. Yani yanarak yüksek ısı yayan flare, bir anlamda sahte bir IR kaynağı oluşturur. Şekil 4.1'de flare atışı yapan bir KC-135R Uçağı görülmektedir.



Şekil 3.5 Flare Atışı

3.2. Elektronik Harpte RF Teknolojisi Kullanımı

3.2.1. Radar ikaz alıcıları

Radar, güdümlü füze ve silah sistemlerini tespit ve teşhis eden sistemlerdir, 2.1.1. bölümünde açıklanmıştır.

3.2.2. RF karıştırıcılar

Karıştırma genel olarak, tehdidin EM spektrumunu kullanmasına engel olmak, zarar vermek veya kısıtlamak amacıyla, EM enerjinin yayınlanması, yeniden yayınlanması veya yansıtılması olarak tanımlanır. Radarlara karşı uygulanan karıştırmanın amacı algılanmayı engellemek veya kısıtlamaktır.

Radarlar, hedefe doğru bir darbe dizini gönderdikten sonra, hedeften yansıyan sinyallerin geliş zamanlarında alıcı sistemlerini aktif hale getirerek, hedef hakkında bilgi üretmeye çalışırlar. Bunun için radardan gönderilen darbe dizinin ne kadar sürede dönmesi gerektiği yaklaşık olarak hesaplanır ve bu zamanlar dışında radara ulaşan darbeler, alıcı devreler tarafından işleme alınmaz. Alıcı devrelerin aktivasyon süresi, gönderilen darbenin genişliğinden küçük olmamak suretiyle üretilen 2 adet darbenin toplam süre kadardır. Bu iki darbe birbirleriyle ardışıktır ve kapı olarak adlandırılır. Anılan kapılar, radarın tipine göre mesafe kapısı veya hız kapısı olarak adlandırılabilir. Radar, tespit ettiği hedefi izleyebilmek için, bu iki kapıya düşen sinyal güçlerini sürekli karşılaştırarak, güçler arasındaki fark sıfır oluncaya kadar kapılarını hareket ettirmektedir. İki kapı arasındaki güç farkı sıfır olduğunda radarın aydınlatması tam hedefin üzerindedir.

İşte karıştırma, radarların çalışma yöntemlerindeki bu zafiyet kullanılarak yapılır. Radar alıcı devreleri hedeften dönen darbeleri beklerken, tam da bu anlarda hedeften dönen eko sinyalinin daha büyük güçte karıştırma sinyalleri gönderilmek suretiyle, radarın kapılarını karıştırma sinyallerine göre hareket ettirmesi sağlanmış olur ve böylece radar karıştırılmış olur.

Gürültü karıştırması

Radarların çalışma prensibi gönderdikleri RF sinyallerin hedeften yansımalarını alarak bu sinyalleri işlemektir, ancak ortamda hedeften başka bir çok şeyden yansıyan ekolar da radara ulaşır. Radarlar algılama seviyesini ayarlayarak clutter etkisinden kurtulmaya çalışırlar. Bu durum radarlar için bir zafiyet yaratır. Eğer

radara hedeften dönen eko işaretinden daha güçlü bir karıştırma işareti gönderilirse, radar kendi işaretini gürültü olarak ve karıştırma işaretini de kendi işareti olarak algılayacaktır. Türleri; Nokta Karıştırması (Spot Jamming), Baraj Karıştırması (Barrage Jamming), Tarama karıştırması (Sweep Jamming)'dır. Bunlar sırasıyla aşağıda açıklanmıştır.

Nokta Karıştırması

Karıştırma, karıştırma cihazının tüm gücünü aynı anda sadece tek bir frekansa karşı yöneltmek suretiyle karıştırma cihazının etkinliğinden ve menzilinden azami şekilde istifade edilmesini sağlayan karıştırma yöntemidir. Karıştırma, uygulanan frekanslara yakın değerdeki frekanslarda çalışan dost silah sistemlerinde daha az girişime neden olur. Bu tür karıştırmanın, hedeflenen almaçlar basit bir frekans değişikliği ile karıştırmanın etkisinden kurtulması, karıştırılacak her hedef frekansı için ayrı bir karıştırıcıya ihtiyaç duyulması nedeniyle ekonomik olmaması, karıştırıcı frekansın sabit tutulmasındaki hassasiyetin fazla olması gibi dezavantajları vardır.

Baraj Karıştırması

Tespit edilen frekans bandı dahilindeki tüm frekansların karıştırılmasına olanak veren karıştırma yöntemidir. Aynı anda birden fazla frekansın karıştırılabilmesine olanak verdiği için ekonomiktir. Düşmanı geniş bir frekans bandını kullanmaktan mahrum eder. Bu tür karıştırmanın; büyük çıkış gücüne ihtiyaç göstermesi, karıştırmadan dost frekansların etkilenebilme ihtimalinin fazla olması, karıştırılacak frekans başına düşen gücün azalması ve bu nedenle karıştırma cihazının ve karıştırma mesafesinin azalması gibi dezavantajları vardır.

Tarama Karıştırması

Karıştırma cihazının belli bir frekans bandını tarayarak karıştırdığı ve tekrar başa dönerek aynı işlemi devamlı olarak yenilediği karıştırma yöntemidir. Bir karıştırıcıyla, birden fazla hedef frekansın karıştırılmasına olanak verir. Karıştırıcı,

çıkış gücü bölünmeden geniş bir frekans bandındaki frekanslara uygulanmış olur. Yapıları çok daha karmaşık olup hedef sistemle ilgili daha fazla bilgiye ihtiyaç gösterir. Bu tür karıştırmada; herhangi bir hedef frekansı üzerinde devamlı karıştırma sağlayamaması, iyi bir frekans planlaması yapılmaması durumunda karıştırılan frekans bandındaki dost sistemlerini de etkilemesi, band içindeki sistemlerin tarama periyodu süresi dışında serbest kalması ve faaliyetlerini sürdürebilmeleri gibi dezavantajları vardır.

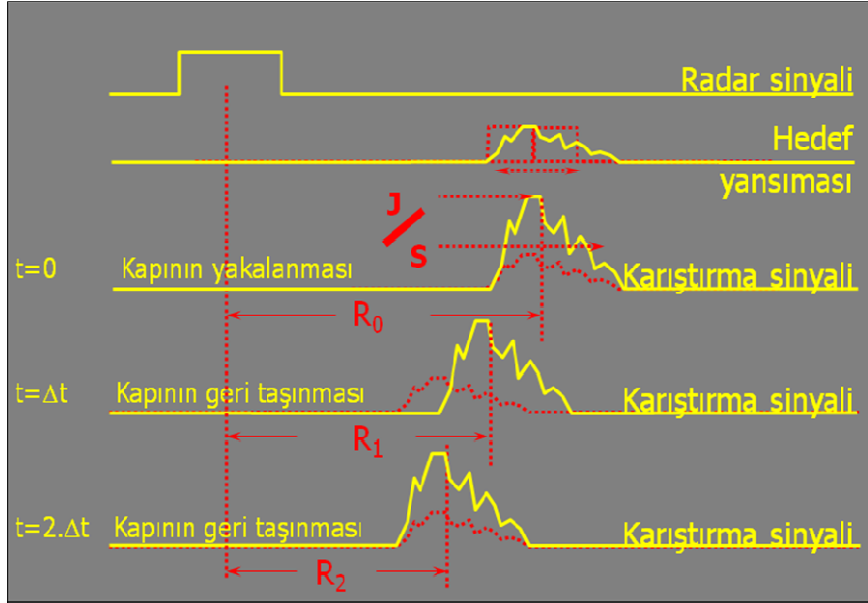
Aldatma karışırması

Aldatma karışırması, radarın elde ettiđi yankı iřaretini yanlış yorumlaması amacıyla, yankı iřareti yerine yankı iřaretine çok benzeyen fakat bazı parametreleri deđiřtirilmiř bir sinyalin radara gönderilerek, radarın yanlış bilgi üretmesinin sađlanmasına aldatma karışırması denir. Aldatma karışırması için, tekrarlayıcı cihazlar kullanılır ve 2 yolla yapılır. Bunlardan birincisi; Radardan alınan iřaretin mesafe, yön, darbe sayısı ve darbe řiddeti gibi parametrelerinden birinin veya bir kaçının tekrar gönderilmesi yoluyla yapılan *hileli aldatma*dır. İkincisi ise tekrarlayıcı cihazlar, radar eko parametrelerinde deđiřiklik yapmaksızın benzer özelliklere sahip yeni darbeler üreterek sahte hedefleri ürettiđi *taklit aldatması*dır. Arama ve gözetleme radarlarına karşı taklit aldatma, atıř kontrol, füze güdüm ve hedef takip radarlarına karşı hileli aldatma uygulanır.

Mesafe Aldatması (Range Gate Pull-Off – RGPO)

Darbe Doppler radarları, hedefin mesafesini izlemek için mesafe kapısı (Range Gate) kullanır. Menzil aldatma karışırması, menzil kapısı devrelerinin zafiyetinden yararlanarak yapılır. Radardan arka arkaya gelen darbeler alınarak, bu darbelerin genliđi arttırılarak belirli bir miktar zaman gecikmesi ile radara geri gönderilir. Radar gönderilen bu aldaticı sinyali kendi sinyali zannederek mesafe kapısını aldatma sinyali üzerine oturtur. Böylece mesafe kapısı uçak üzerinden sahte bir hedefe dođru çekilmiř olur ve farkında olmaksızın radar gerçek hedefin takip yeteneđini kaybeder. Bu nedenle bu aldatmaya mesafe kapısı çekme (Range Gate Pull-Off – RGPO) denir.

Aldatma sinyali kesildiğinde radarın sahte hedefe olan kilidi kırılır, ancak bu anda radar aldatıldığını anlayabilir. RGPO tekniği, tracking radarlarına karşı etkili bir tekniktir. Mesafe aldatması radarın otomatik kazanç kontrol (Automatic Gain Control-AGC) devrelerinin zafiyeti sayesinde yapılabilir. RGPO yapılabilmesi için öncelikle gelen radar sinyali kaydedilir, kaydedilen sinyal kullanılarak gelen sinyal parametreleriyle aynı parametrelere sahip fakat daha güçlü bir sinyal oluşturularak geri gönderilir. Bu sinyal, radarın AGC devreleri tarafından farkedildikten sonra, mesafe kapısının çalınması için yavaş yavaş geciktirilerek gönderilmeye başlanır. Gecikme en yüksek değere geldiğinde mesafe kapısının çalınma periyodu tekrarlanır. Şekil 3.6’da radar mesafe kapısının RGPO tekniği kullanılarak nasıl çekildiği gösterilmektedir.

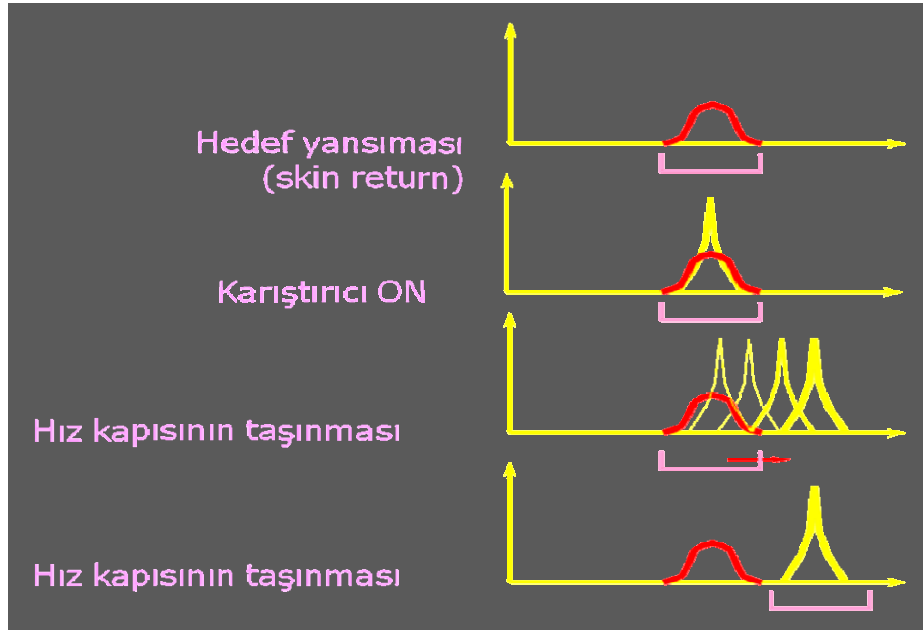


Şekil 3.6 RGPO Tekniği

Hız Aldatması (Velocity Gate Pull-Off – VGPO)

Darbe Doppler radarları, hedefin hızını izlemek için hız kapısı (Velocity Gate) kullanır. Hız aldatması da, menzil aldatmasında olduğu gibi izleme devrelerinin zafiyetinden yararlanır. Radardan gelen darbeler alındıktan sonra yükseltilerek yapay doppler kayması yaratılarak tekrar gönderilir. Radar gönderilen bu darbeleri kendi

darbeleri sanarak işler ve hedefin hızında bir artış olarak değerlendirir. Böylece, hız kapısı hedefin gerçek hız kapısından farklı kapılara çekilmiş olur. Hız aldatması için uygulanan bu yönetime hız kapısı çekme (Velocity Gate Pull-Off – VGPO) denir. En yaygın çekme 2 şekilde yapılır; bunlar doğrusal ve parabolik çekmedir. Hız kapısı çalınma ya da hız yanıltması CW ve darbe radarları gibi dopler tekniği kullanan radarlara karşı etkili bir ECM tekniğidir. Bu teknik gelen radar sinyallerinin frekansında kaymalar yaratarak geri gönderilmesi gerçekleştirilir. Doppler filtresinin içerisine hedeften yansıyan sinyalin de girmesi için, başlangıçta frekans kayması programlanır. Böylece radarın AGC devrelerinin karıştırılması mümkün hale gelir. Daha sonra tekrarlanan sinyalin frekansı yavaş yavaş radarın maksimum doppler frekansına doğru çekilir. Maksimum değerden sonra karıştırma sinyali kesilir. Böylece radar tekrar kilit atmak için arama moduna geçer. Şekil 3.7 VGPO Tekniği kullanılarak hız kapısının taşınması gösterilmektedir.

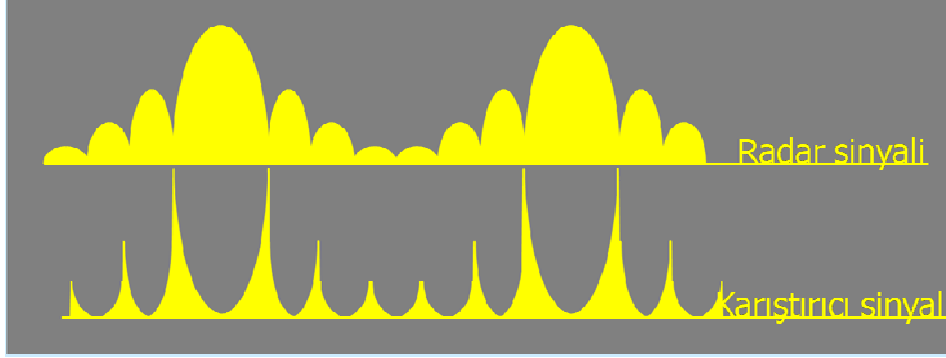


Şekil 3.7 VGPO Tekniği

Açı Aldatması (Angel Walk-Off)

PD radarlarından gelen darbeler alınıp, gerçek genliklerine zıt darbeler kullanılarak yankı zayıflatılırken, karıştırma işaretleri ile radarın algılama açısı değiştirilir. Açı

aldatması amacı ile uygulanan bu y nteme a ı kaydırma (Angel walk-off) olarak adlandırılır. Karıřtırma iřareti kesilince radar kilit kıracaktır. Radarın hedefi her yakalayışında bu iřlem tekrar edilir. řekil 3.8’de a ı aldatmasının radar sinyaline nasıl uygulandığı g sterilmektedir.



řekil 3.8 A ı Aldatması

Tekrarlayıcı Aldatması (Repeater Jamming)

PD radarlarından gelen darbeler alınıp,  ok sayıda sahte hedef yaratacak řekilde yapay eko iřaretleri g nderilerek taklit yoluyla radar aldatılır. Yani radar skobunda tek bir hedef yerine  ok sayıda hedef g z kmesi saėlanır.

Chaff/Decoy Kullanımı

Chaff Kullanımı

Chaff, tehdit radarının g r ř alanına, tehdit  zelliklerine g re hazırlanmış y ksek genlikte yansımalar yaratacak iletken cisimlerdir ve bi imleri řekil 3.9’da g sterilmiştir.



Şekil 3.9 Chaff Kullanımı

Bu cisimler Şekil 3.10’da gösterilen bir atma sistemi ile atılarak bir chaff bulutu oluşturulur. Uçak bu bulutun arkasında gölgelenir, bu sırada uçak manevra yaparak radar kilidini kırar. Chaff’ın kullanım şekilleri aşağıda verilmiştir.



Şekil 3.10. Chaff/Flare Atma Sistemi

Chaff’ın kullanım şekilleri aşağıda verilmiştir.

Chaff Korunması

Uçak, chaff’ın yayılımı ile oluşan chaff bulutunun arkasında gizlenerek, uçağın manevra yaparak kaçışına imkan sağlanır.

Chaff Aldatması

Farklı mesafelerde atılan Chaff'lerin havada yayılımı ile tehdit radarlarına birden çok hedef gösterilir ve asıl hedef gizlenir.

Radarın Satüre Edilmesi

Radar sistemine çok fazla noktadan yüksek genlikte yansıma ulaşması sağlanarak izleme sistemi bloke edilir.

Koridor Açma

Uçaklar yoğun chaff'la kaplanmış bir alandan geçirilerek radarlar tarafından tespit edilmeleri engellenir.

Aktif Sahte Hedef (Decoy) Kullanımı

Tehdit radarının görüş alanına, paraşüte bağlanmış (veya UAV), ucuz ve harcanabilir sahte hedef maksatlı sinyal kaynakları atmak suretiyle radarın/füzenin uçak yerine sahte hedefe angaje olmasını sağlanır, 2 tipi mevcuttur.

Tam Aktif Decoy

Bu decoy, radar sinyalini algılayarak o sinyali yan loblardan yüksek kazançla tekrarlayan aktif decoy tipidir ve şekli Şekil 3.11'de verilmiştir.



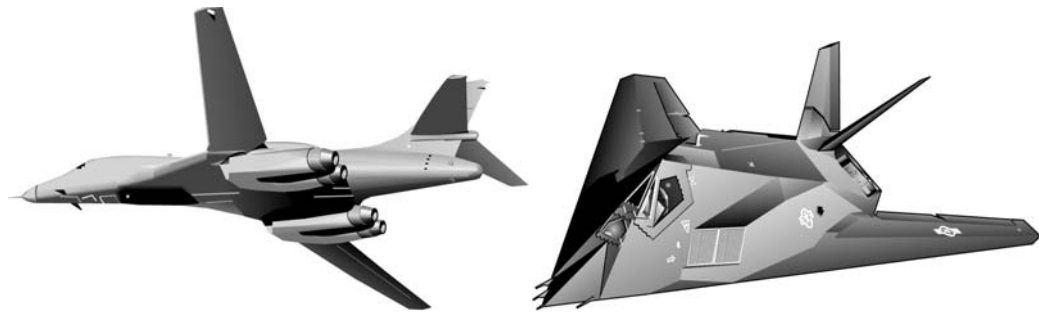
Şekil 3.11. Sahte Hedef

Yarı Aktif Decoy

Chirp modülasyonlu (zamanda artan veya azalan frekans) sinyal göndererek radarda hatalı Doppler kayması yaratan, tekrarlamayan türde olan tipidir.

3.2.3. Görünmezlik (Stealth) teknolojisi

EM ve fiziksel özelliklerin değiştirilerek dost birimlerin tespit edilebilirliğinin azaltılması olarak bilinir. Şekil 3.12 Görünürlüğü Azaltılmış Uçaklar görülmektedir.



Şekil 3.12 Görünürlüğü Azaltılmış Uçaklar

Görünürlüğü azaltmak için uygulanan yöntemler aşağıda sunulmuştur.

Hedefin şeklinin düzeltilmesi

Hedefin küçük eğrilik yarıçaplı (radius of curvature) olarak ve herhangi bir kenara sahip olmayacak şekilde tasarlanmasıdır.

Antiradar kaplayıcılar

Hedefin yüksek yansıma yapan bölgelerini, gelen dalgayı soğuracak materyaller ile kaplanmasıdır.

Dalgaların yönlendirilmesi

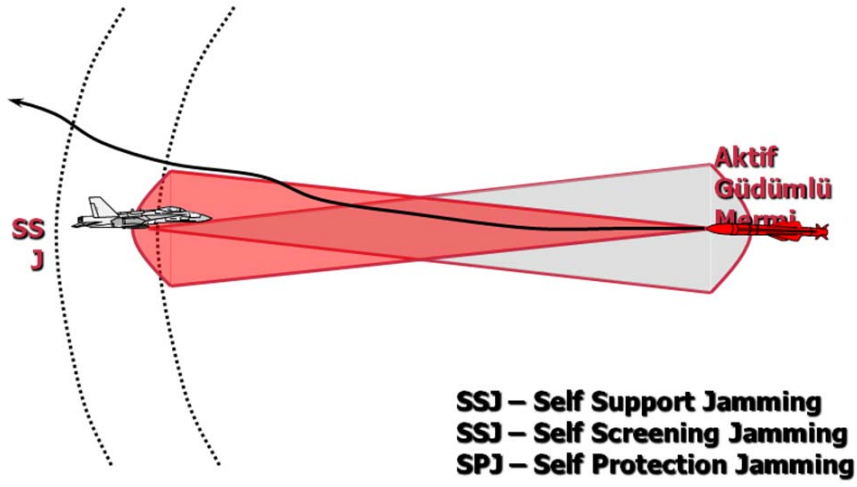
Hedefin şeklini, dalgaların geldikleri yönden farklı yönere yansımaları sağlayacak şekilde düzenlenmesidir.

3.3. Karıştırma Yöntemlerinin Harekatta Kullanım Konseptleri

Harekat ortamında, bir bölge birden çok sistem ile korunmakta ve benzer biçimde bir bölgeye taarruz edilirken birden çok uçak göreve gönderilmektedir. Bu bir çok tehdit ve uçaktan oluşan operasyon bölgesinde, başarı oranını arttırmak için EH karıştırma yöntemlerinin taktiksel olarak uygulanması gerekmektedir. Bu uygulamalarla ilgili olarak; korunma karıştırması, refakatte karıştırma ve uzaktan karıştırma olmak üzere 3 ayrı kullanım konsepti belirlenmiştir.

3.3.1. Korunma karıştırması (Self Screening Jamming – SSJ)

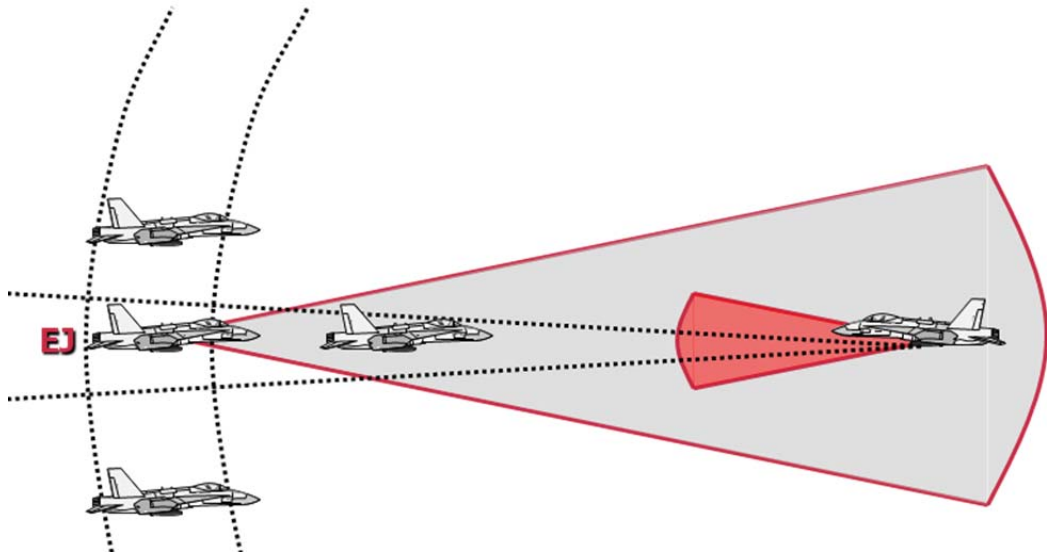
Bir radarın hedefi durumundaki uçağın, kendisinin algılanmasını engellemek amacıyla, bu radara karşı yaptığı karıştırma işlemi Korunma Karıştırması olarak adlandırılır ve Şekil 3.13'te bir uçağın kendisine yaklaşan güdümlü bir mermiye karşı kendini koruması gösterilmektedir. Korunma karıştırması amacıyla, gürültü veya aldatma karıştırması kullanılabilir.



Şekil 3.13 Kendini Koruyan Uçak

3.3.2. Refakatte karıştırma (Escort Jamming – EJ)

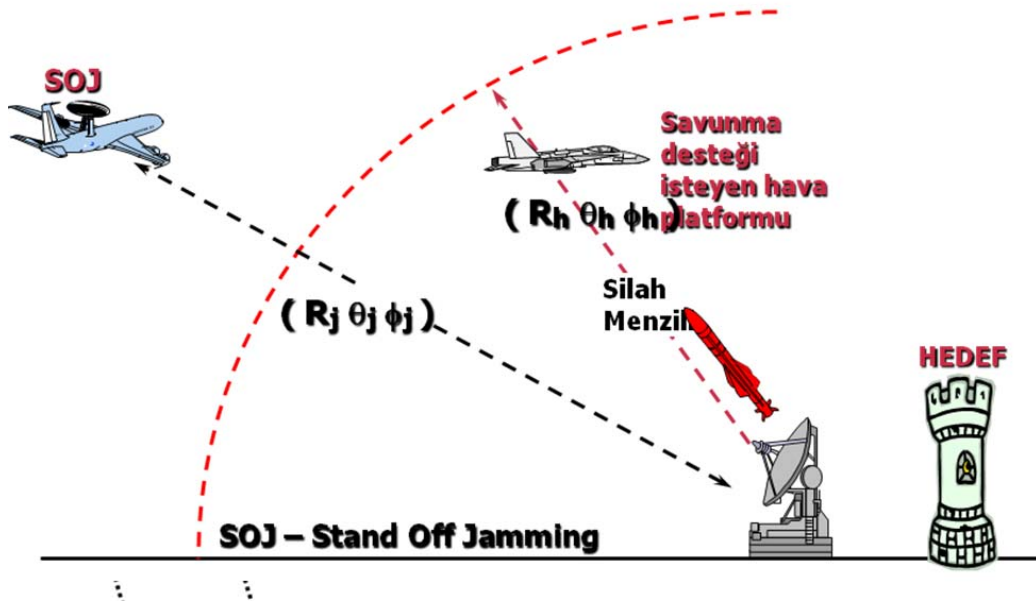
Bir radarın hedefi durumundaki uçağın algılanmasını engellemek amacıyla, hedefin yakın kolunda uçan diğer bir uçak tarafından, radara karşı yapılan karıştırma işlemine eskort karıştırması adlandırılır ve Şekil 3.14’te eskortluk yapan uçağın, önündeki uçağı nasıl koruduğı gösterilmektedir. Eskort karıştırma amacıyla, grlt veya aldatma karıştırması kullanılabilir.



Şekil 3.14 Refakatte Karıştırma

3.3.3. Uzaktan karıştırma (StandOff Jamming - SOJ)

Hedef durumunda bulunan uçakları destekleyen düşman hattının gerisinde duran EH taaruz uçaklarının, destekledikleri uçakların bir radara uyguladıkları karıştırma işlemine uzaktan karıştırma denir ve uygulanma biçimi Şekil 3.15'te gösterilmiştir. Uzaktan karıştırma amacıyla genellikle gürültü karıştırması kullanılır.



Şekil 3.15 Uzaktan Karıştırma

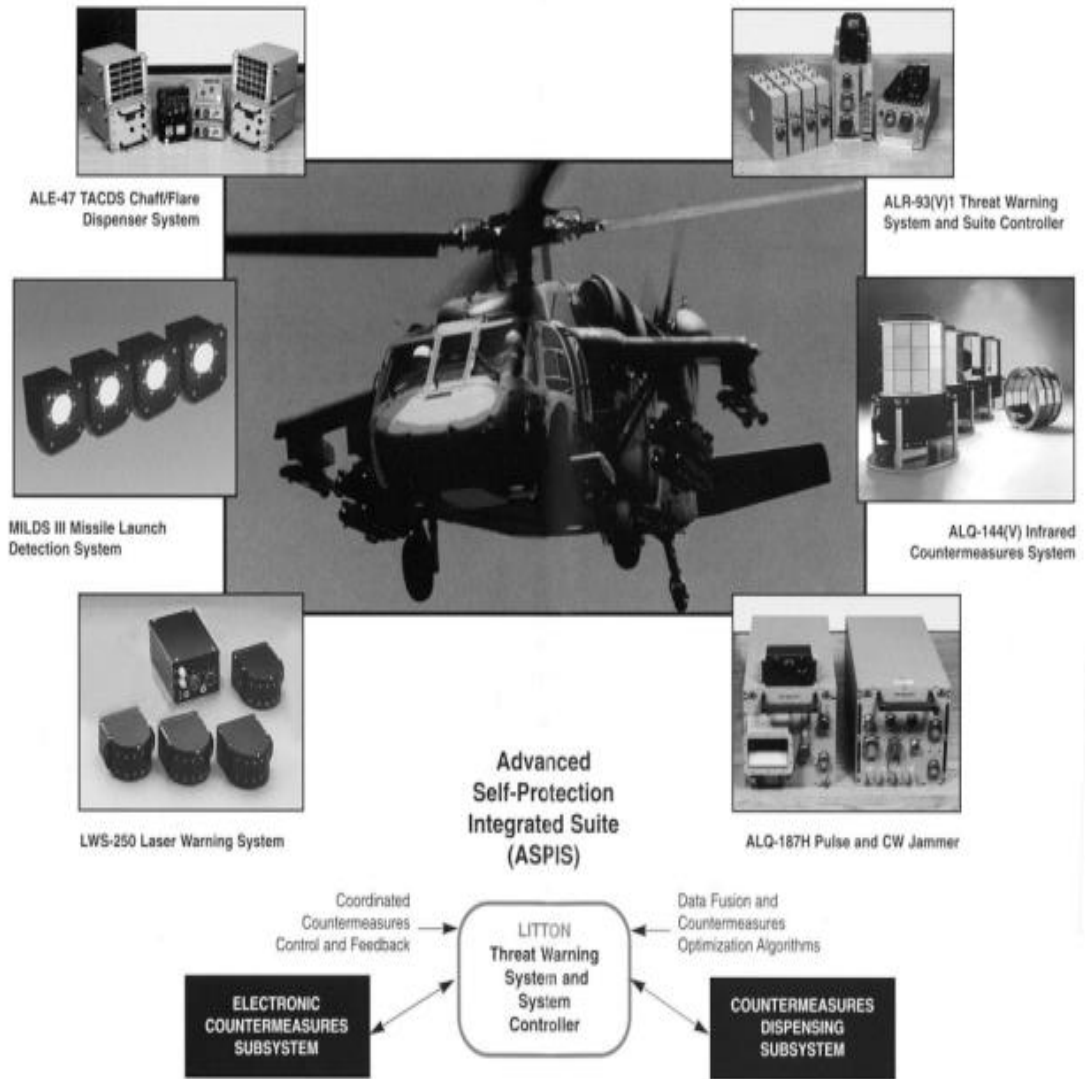
3.4. Hava Platformlarında Tümüleşik EW Suite Sistemleri

Günümüze kadar geçen süreçte, teknolojiye hızlı gelişmelerle birlikte artan silah sistemleri nedeniyle, bir hava platformu, ancak birden çok, elektronik harp sistemi kullanılarak korunması mümkün olmuştur. Özellikle RF, IR ve lazer güdümlü, yerden havaya ya da hava-hava füzeler uçaklar için çok ciddi tehdit oluşturmaktadır. Öte yandan yerde konuşlu, hedefi takip ederek hedefe füze ve mermi atabilen silah sistemleri uçakları tehdit etmektedir.

Bir uçağın gönderildiği operasyon bölgesinde görevini yaparken bekasını da sürdürebilmesi için, tüm bu tehdit ortamındaki tehditlere karşı korunabilmesi gerekmektedir. Operasyon bölgesinde tehditlerin çeşitliliğine karşı uçağı koruyabilmek için, birden çok EW sisteminin uçak üzerine yerleştirilmiş olması gerekmektedir. Örneğin, bir hava platformu üzerinde, Radar Warning Receiver- RWR, Missile Warning System-MWS, Laser Warning Receiver- LWR, RF karıştırıcılar, IR ve/veya UV karıştırıcılar, Chaff-Flare Atma Sistemi, çekilebilir sahte hedef sistemleri bir arada kullanılabilmektedir.

Bir uçak üzerinde birden çok çeşitte EW Sistemi olsa bile, tüm EW sistemlerinin tek bir görevi vardır, uçağın bekasını sağlamak. O halde farklı yapılarıdaki bu sistemlerin birbirleriyle uyumlu ve birbirlerini destekler yönde çalışmaları gerekmektedir. Örnek olarak ikaz sistemleri, karıştırıcı sistemlere hedefin mesafe, yön bilgilerini hassas biçimde sağlamalıdır. Öte yandan karıştırıcı sistemler karıştırma yaparken, ikaz sistemleri bu karıştırmadan olumsuz etkilenmemelidir.

Uçak, tehdit ortamına girdiğinde, ortamda tehdit sayısı çok ve tehditler çeşitli yapıda olabilir. Operasyon bölgesinde görevin başarı ile icra edilebilmesi için, EW sistem kaynaklarını tehditlere paylaştırarak çok sınırlı zaman içinde en etkili tekniğin uygulanması gerekir. Bu ise sistemlerden sürekli akan tehdit bilgilerinin değerlendirilerek, eldeki kaynakların çok hızlı bir biçimde tahsis edilebilmesi ile mümkün olur. Bir füzenin fırlatıldıktan sonra ortalama uçuş süresinin 5, 6 saniye olduğu düşünülürse, tehditten gelen verilerin değerlendirmesinin, platformu kullanan ve EW dışında bir çok sistemi kontrol eden pilot tarafından manuel olarak yapılması mümkün olmamaktadır. Bu nedenle RWR, MWS ve LWR sisteminden gelen bilgiler değerlendirilerek, tespit edilen tehdide karşı uygulanabilecek en etkili karşı tedbiri belirleme işi, uçaklara EH sistemlerine yönelik konulmuş EW Suite olarak adlandırılan merkezi kontrol birimi tarafından yapılmaktadır. EW Suite, EW sistemlerinin birbirleri ve uçak aviyonik sistemleri arasındaki koordinasyonu sağlamaktadır. Şekil 3.16'da Tümüleşik EW Suite Sistemi uygulanmış bir helikopter görülmektedir.



Şekil 3.16. Tumbleweed EW Suite Sistemi

4. DRFM (DIGITAL RADIO FREQUENCY MEMORY) TEKNOLOJİSİ

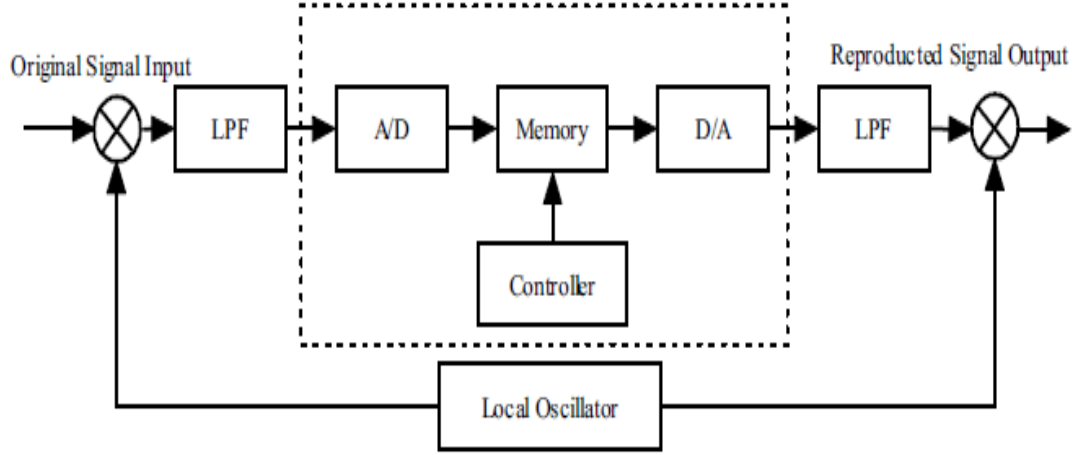
Yakın geçmişte radarları aldatabilmek için, radardan gelen dalga formunu kaydetmek üzere “Frequency Memory Loop-FML” adı verilen sistemler kullanılmaktaydı. Bu sistemler analog olmakla birlikte, kayıt yöntemi, gelen dalga formunu geciktiricilerden geçirilerek, gelen sinyalin zaman geciktirmesi ile geri gönderilmesi esasına dayanıyordu. Ancak, bu cihazlar tutarlılık kontrolü (Coherency Check) yapan radarlara karşı etkili olamıyorlardı. FML’lerin uzun süre gelen dalga formunu saklayamamaları ve ürettikleri karıştırma sinyallerinin radarlar tarafından ayırt edilebilmesi, bu konuda yeni araştırmaların yapılmasına neden oldu. Araştırmalar sonucunda, dalga formunu geldiği biçimde saklayabilecek ve istenilen parametreler değiştirildikten sonra aynı formda tekrar gönderebilecek DRFM teknoloji geliştirildi.

Bu bölümde DRFM’in tanımı ve kapsamı verildikten sonra, günümüzde kullanılmakta olan DRFM’lere ilişkin tanımlar verilecek ve DRFM uygulamasına geçilecektir.

4.1. DRFM’in Tanımı ve Kapsamı

DRFM Mikrodalga ve RF sinyallerin yüksek hızlı örnekleme ile dijital bir hafızada saklanması için kullanılan bir tekniktir. DRFM teknolojisi ile, RF sinyallerini kopyalamak ve bu sinyallerin bazı parametrelerini değiştirerek yeniden geri gönderilmesiyle düşman radar sistemlerinin aldatılmasına olanak sağlanır. DRFM teknolojisinin en önemli avantajı; Tutarlılık Kontrolü (Coherency Check) yapan bazı radarların da aldatılabilmeleridir. Tutarlılık kontrolü yapabilen radarlar, kendi eko sinyallerini, sıradan tekrarlayıcılar kullanılarak üretilen karıştırma sinyallerinden ayırt ederek, aldatılmaya çalışıldıklarını algılayabilirler. Karıştırılmaya çalışıldığını fark eden radar, mod değiştirerek ya da Electronic Counter Counter Measure (ECCM) özelliklerini devreye sokarak karıştırıcı sistemin etkilerinden kurtulabilir. Bu noktadan hareketle, DRFM teknolojisinde, herhangi bir RF kaynak kullanılarak

karıştırma sinyali üretme yerine, sinyalin aynısı kaydedilerek tekrar gönderilir. Böylece gelişmiş radar, eko sinyali ile karıştırma sinyalini birbirinden ayırt edemez. Şekil 4.1’de temel bir DRFM Sisteminin blok diyagramı gösterilmiştir [9]. Gelen RF



Şekil 4.1 DRFM Blok Şeması

sinyal düşük bir frekansa düşürüldükten sonra sayısala çevrilerek örneklenir, örneklemeleme karşılık gelen sayılar yüksek hızlı hafızaya kaydedilir. Kaydedilen sinyalden yeni bir tutarlı sinyal yaratmak için, kaydedilen sinyal analoğa çevrildikten sonra üst bir frekansa çevrilerek yayınlanır.

DRFM Sisteminin anlık band genişliği öncelikle Analog/Digital çeviricinin örnekleme oranına bağlıdır. Yüksek hızlı sayısal hafıza, hem kayıt hem de kayıttan yeni bir sinyal oluşturmak için çift portlu olmak durumundadır. Hatta hem kayıt ve aynı anda kayıttan sinyal oluşturabilen çok portlu hafızalar bir çok uygulamada tercih edilmektedir. Kayıt yapma ve kayıttan yeni sinyal oluşturabilme özelliklerinin yanında DRFM’ler aynı zamanda sinyal işleme özelliklerine de sahiptirler. Sinyal işleme uygulamaları analog formda elektronik ya da sayısal olarak gerçekleştirilebilir.

Günümüzde DRFM’in en önemli uygulama alanları elektronik karıştırma amaçlı sahte radar sinyalleri yaratarak hedefin aldatılmasıdır.

Radar sinyalinin örneklenmesi, DRFM sinyali içinde harmoniklerin oluşmasına neden olur. Bu harmonikler takip eden radar tarafından ortamda DRFM karıştırma sinyalinin var olup olmadığının belirlenmesinde kullanılabilir. Harmoniklerin genliklerinin büyüklükleri DRFM sinyalinin tespit edilmesinde etkili olacaktır ve harmoniklerin genliklerinin büyüklüğü analog digital çeviricilerin örnekleme büyüklüğüne bağlıdır.

DRFM sistemine ulaşan sinyalin $x(t)$ olduğunu kabul edersek, RGS operasyonu sonrası elde edilen çıkış sinyali $y(t)$;

$$y(t) = x(t - c(t)) \quad (7.1)$$

Burada $c(t)$, DRFM sistemine ulaşan sinyal ile DRFM sisteminden tekrar gönderilen sinyal arasındaki zaman gecikmesini belirleyen zaman gecikme fonksiyonudur. İdeal olarak, lineer RGS'nin zaman gecikme fonksiyonu, lineer ve zamanın sürekli fonksiyonudur. RGS zaman gecikme fonksiyonu;

$$c(t) = C_i(t) = \alpha t \quad (7.2)$$

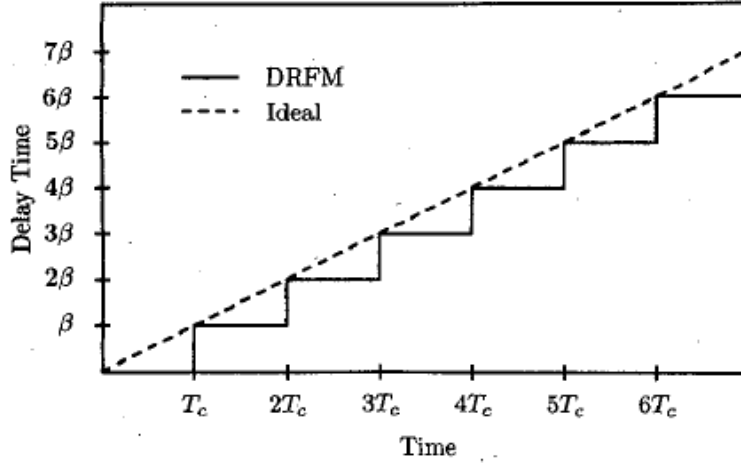
yukarıda α gecikme oranı (pul-off) dır. Kesikli zaman sistemlerinin doğası nedeniyle, DRFM tabanlı Elektronik Taarruz sistemlerinin lineer ideal zaman gecikme fonksiyonu, merdiven basamağı şeklinde modellenmek zorundadır. Bu nedenle RGS bazlı DRFM'in zaman gecikme fonksiyonu [8];

$$c(t) = c_d(t) = \beta \sum_n u(t - nT_c) \quad (7.3)$$

Burada,

$$u(t) = \begin{cases} 1; & \text{if } t \geq 0, \\ 0; & \text{otherwise.} \end{cases} \quad (7.4)$$

Ayarlandıktan sonra, Şekil 7.2’de ideal lineer bir RGS’nin zaman gecikme fonksiyonu gösterilmektedir.



Şekil-4.2 DRFM’in Lineer RGS’si için zaman gecikme fonksiyonu

Zaman çözünürlüğü, RGS güncelleme oranı ve lineer RGS parametresi α tarafından basamak sayısı (β) ve basamak genişliği (T_c) ile belirlenir. DRFM’in zaman gecikmesi çözünürlüğü (t_d) ve güncelleme oranı (t_s), hedefin ve seçilen radarın gerçek parametrelerine göre ayarlanır. Zaman gecikme çözünürlüğü, her bir hedef darbesi güncellemesinde, radarın mesafe takip kapısının dışına çıkmasını engelleyecek biçimde seçilir. Zaman gecikme çözünürlüğü bir değere ayarlandıktan sonra, hedefin maksimum mesafe oranını ya da pull of rate’ini sağlamak üzere güncelleme oranı ayarlanır. ($\alpha_{max}=t_d/t_s$). Buradan hareketle, genel olarak, karşılaştırılan hedefin mesafe takip kapısının dışına çıkmasını engellemek için $\beta=t_d$ olmalıdır ve $\beta/T_c \leq \alpha$ olması için T_c , t_s ’nin birkaç katı olmalıdır. Buradan;

$$T_c = [t_d/(t_s \alpha)] t_s \quad (7.5)$$

Darbe radarlar için, DRFM’e gelen giriş sinyali darbe dalga formunda sinüs ile modüle edilmiş bir sinyaldir. Darbe tekrarlama frekanslarında spektrum şeklinin bozulmaması ve spektrumun kopyalarının oluşmaması için darbe dalga şekli

kullanılmayacaktır. Böylece DRFM'e gelen giriş sinyali sinüzoidal ve lineer RGS'nin çıkışı,

$$y(t) = e^{j2\pi f_0 (t - \beta \sum_n u(t - nT_c))} \quad (7.6)$$

$$y(t) = \underbrace{e^{j2\pi f_0 t}}_{\text{taşıyıcı}} \underbrace{e^{-j2\pi f_0 \beta \sum_n u(t - nT_c)}}_{\text{faz değişimi}}$$

olarak verilebilir. Burada “fo” radarın gönderme frekansıdır. Kesikli zaman gecikmesi giriş sinyalinin fazında bir değişime neden olur. Güncelleme periyodu başına fazdaki değişim;

$$\Delta\phi = -2\pi(f_0\beta - [-2\pi f_0\beta] + [f_0\beta]) \quad (7.7)$$

Bu faz kayması her Tc başına olacağından, faz kayma frekansı aşağıdaki gibidir.

$$f_s = \frac{\Delta\phi}{2\pi\Delta t} = \frac{-(f_0\beta - [-2f_0\beta] + [f_0\beta])}{T_c} \quad (7.8)$$

Çıkış sinyalini aşağıdaki formda yazarsak,

$$y(t) = \sum_n p_n(t)\delta(t - nT_c) \quad (7.9)$$

ve fourier transformunu alacak olursak,

$$\sum_n \delta(t - n_c T) \Leftrightarrow 1/T \sum_n \delta(f - m/T) \quad (7.10)$$

Şeklinde olur. DRFM lineer RGS'nin, fc=1/Tc'lerde harmonikler oluşacaktır. Böylece DRFM spekturumunda,

$$f = f_0 + f_s \pm n f_c \quad (7.11)$$

Frekanslarında spektral çizgiler oluşacaktır. Burada “n” tamsayıyı göstermektedir.

4.2. Günümüzde Kullanılmakta Olan DRFM'lere İlişkin Tanımlar

Günümüzde kullanılmakta olan DRFM'lere ilişkin tanımlar aşağıda verilmiştir [3].

4.2.1. Anlık band genişliği (Instantaneous Bandwidth- IBW)

Anlık band genişliği; aldatma sinyalini henüz oluşturmada, DRFM girişine herhangi bir anda gelen tüm RF giriş sinyal frekanslarının kapsandığı ve bu sinyallerin sayısala çevrildiği, kayıt edilebildiği ve sistemin hiçbir anahtarlama ya da ayarlama yapmaksızın giriş sinyalini geri çağırabildiği aralıktır. Bir DRFM'in IBW'si sistemin örnekleme zaman oranına ve hafıza kapasitesine göre değişir. Dijital teknolojiye kısıtlamalar nedeniyle, analog sayısal çeviriciler ve ilişkili devreler maksimum 1GHz saat frekansı ile çalışabilmektedirler. Bu nedenle, günümüzde 500 MHz'lik IBW'e sahip DRFM'ler kullanılmaktadır.

4.2.2. Frekans ayar aralığı

Eğer kullanılabilir IBW, ilgilenilen tehdidin band genişliğinden küçük ise, bu takdirde DRFM tehdit frekansını işleyebilir. DRFM'in IBW içerisinde gelen sinyali işleyebilmesi için, tehdit sisteminin kullandığı herhangi bir sinyal spektrumuna yönlendirebilecek lokal osilatörlere sahip bir sisteme ihtiyaç duyulur. Çevirici donanımına bağlı frekans ayar aralığı olarak oktav band genişliğini veya daha büyük band genişliğini kapsamak mümkündür. DRFM aynı anda birden çok tehdidi karıştırmak için de kullanılabilir. IBW içerisine düşen istenmeyen sinyaller ayarlanabilir band durduran filtreler kullanılarak filtrelenebilir, zaman skalasında herhangi bir tehdit seçilerek DRFM içinde saklanan tehditler arasına eklenebilir.

4.2.3. Lokal osilatör ihtiyacı

DRFM içerisinde kullanılacak lokal osilatörler, ihtiyaç duyulan IBW'e, DRFM çıkışında istenilen frekans doğruluğuna ve maksimum depolama zamanına göre belirlenirler. IBW'nin istenen değere ayarlanabilmesi, lokal osilatörün slew oranına ve istenilen frekansa ayarlanabilme zamanına bağlıdır. Benzer biçimde DRFM çıkışının frekans doğruluğu, anlık frekanstaki sabit kalabilme durumuna bağlıdır. Maksimum darbe depolama zamanı, lokal osilatörün büyük band genişliğine sahip sinyallerde band genişliği boyunca sabit çıkış vermesine bağlıdır. Yukarıda anılan özellikleri stabil dielectirik osilatörleri (DSO), sayısal ayarlanabilir voltaj kontrollu osilatörler (VCO), kristal osilatör-tarak jenaratörleri ya da frekans sentezleyiciler gibi sabit frekans osilatörleri sağlayabilmektedir.

4.2.4. DRFM duyarlılığı

DRFM'de superheterodyne alıcılara benzer biçimde alt frekans dönüşümü yapıldığından, hassasiyet, band genişliği ve yanlış alarm kavramları benzerdir. Minimum sinyal gürültü oranını (SNR) karşılamak için uygun biçimde RF ve IF kuvvetlendirmesi yapılır. Yanlış alarm oranını kabul edilebilir seviyede tutmak için hesaplanan SNR oranı ile DRFM'in duyarlılığı hesaplanır.

4.2.5. Dinamik aralık

Bir DRFM'in dinamik aralığı, dilimle sırasında kullanılan bit sayısına bağlıdır. Tek bit e sahip DRFM'ler, ilave devrelere ihtiyaç duymaksızın çok bit DRFM'lere göre geniş dinamik aralıklarda çalışabilirler. Çok bit DRFM'ler, geniş aralıkta çalışabilmek için, analog sayısal çeviriciler, hassas giriş sağlamak için otomatik kazanç kontrol devreleri gibi ilave donanımlara gereksinim duyarlar.

4.2.6. Örneklem gereksinimi

DRFM tasarımımda örneklem oranı belirli sınırlar içinde ayarlanabilir bir faktördür. Nyquist örneklem teoremine göre bir sinyal, sinyal içindeki en büyük frekansa eşit ya da içindeki en büyük frekans bileşeninin iki katından daha büyük olacak şekilde örneklendirilmelidir. Ya da örneklem frekansı sinyal band genişliğinin iki katı olmalıdır. Bu nedenle DRFM'in örneklem oranı en azından IBW'nin iki katı olmalıdır. Eğer bu koşul karşılanırsa ilgili sinyalin doğru bir şekilde yeniden oluşturulması mümkün olur. Örneğin, eğer 500 MHz'lık bir IBW isteniyorsa örneklem oranı 1000 MHz'e eşit ya da büyük olmalıdır.

4.2.7. Dilimleme gereksinimi

Analog sayısal çeviriciler, örneklem/dilimlemeyi genlik ya da faza göre yaparlar. Analog sayısal çeviriciler, DRFM'in IBW'si ile uyumlu saat hızında çalıştırılmalıdırlar. Aynı zamanda saat hızı hafıza birimleri ile de uyumlu olmalıdır. Dilimleme, DRFM'in dalga şeklinin güvenilirliği için çok önemlidir. Harmoniklerin bastırılabilirlik düzeyi, seçilen örneklem oranına ve kaç bit dilimleme yapıldığına bağlıdır. Verilen bir örneklem oranı için, dilimleme bit sayısı arttıkça harmonik sinyal seviyesi azalır.

4.2.8. Depolama gereksinimi

DRFM'in hafıza büyüklüğü, kaydedilecek en uzun darbenin darbe genişliği ve IBW ile belirlenir. Kaydedilen toplam bit sayısı (N)

$$N = f_s \cdot N_s \cdot N_b \quad (7.12)$$

Olarak verilir. Burada;

f_s = örneklem oranı = 2 x IBW

N_s = tehdidin maksimum darbe genişliği

N_b = örnek başına bit sayısı

Örnekleme oranı 50 MHz ve A/D'den örnek başına bir bit toplandığını, her 20 nano saniyede bir bit alınabildiğini varsayalım. Eğer bu durumda en uzun darbe 100 mikro saniyede kaydedilebiliyorsa, o zaman depolama için 5000 bit e ihtiyaç duyulur.

4.3. DRFM Uygulamasında Simulink Programı Kullanımı

Bu çalışmada; MatLab Simulink programı kullanılarak ECM sistemlerinin bir alt birimi olan Digital Radio Frequency Memory (DRFM) sistemi simule edilmiştir. Simulasyon kapsamında DRFM'in fonksiyonlarını incelemek üzere, öncelikle temsili bir radar sinyali oluşturulmuştur. Radar sinyali oluşturulduktan sonra, bu radar sinyalinin RWR tarafından tespit edilebildiği ve sinyal parametrelerinin belirlendiği varsayılmıştır. RWR tarafından tespit edilen bu sinyal, aldatma sinyalini oluşturmak üzere DRFM ünitesine gönderilmiştir. Gerçek hayatta kullanılan ECM sistemlerinde, tehdide karşı uygulanacak teknik, merkezi bir birim tarafından belirlenmekte, seçilen tekniğin üretilmesi için teknik geliştirici birime (DRFM) komut gönderilmektedir. Bu çalışmada yapılan simülasyonda, ECM sisteminin diğer birimleri içerilmediğinden, DRFM'e komut gönderilmeksizin, birden çok sahte hedef yaratma, RGPO ve VGPO karıştırma tekniklerinin üretilmesi sağlanmıştır.

DRFM simulasyon programı, Simulink programı kütüphanesinden seçilen bloklar kullanılarak yapılmıştır. Kullanılan bloklarla ilgili olarak aşağıdaki kısa bilgiler sunulmuştur.

4.3.1. Sayısal faz modülasyonu (Phase Shift Keying-PSK)

PSK, faz modülasyonu, frekans modülasyonuna çok benzemektedir. PSK'da gönderilen dalga şeklinin frekansı yerine fazında bir değişiklik yapılır. Fazın değiştirilmesi ile gönderilecek sayısal bilgi temsil eder. Faz modülasyonlu dalga formu, eşit frekanslı, ancak birbirinin tam tersi faza sahip iki sinyalin sayısal bilgisinin değiştirilmesiyle oluşturulur. Eğer dalga formu bir cosinüs dalga formu ile modüle edilirse, bu durumda iki bileşen oluşur. Bunlardan birisi alınan frekansın iki katı olan cosinüs dalga formudur. Diğeri ise cosinüs dalga formunda oluşan faz

kayması ile orantılı olarak genliği değişen bağımsız frekans terimidir. Böylece yüksek frekans terimi filtrelenerek gönderimden önce orijinal modüleli bilgi elde edilmiş olur. Konsept olarak PSK'nın grafiksel olarak resimlenmesi oldukça güçtür, fakat matematiksel olarak modellenmesi mümkündür.

4.3.2 QPSK (Quadrature Phase Shift Keying)

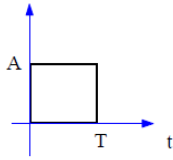
QPSK, PSK'nın geliştirilmiş şeklidir. PSK'da 1 bit ile 2 faz temsil edilirken, QPSK ile taşıyıcı frekansı 4 farklı faz kaymasına maruz kalır ve 2 bitlik bilgi ile temsil edilir. 2 bit ile 4 farklı faz tanımlamak mümkündür.

$$s_i(t) = A_c p_s(t) + \cos(2\pi f_c t + \frac{2\pi i}{M}) \quad (8.1)$$

Burada $p_s(t)$ dalga şekil fonksiyonudur.

$$\theta_i = \frac{2\pi i}{M} \quad (8.2)$$

faz terimidir. Bu terimden de görüleceği gibi bir periyotta cosinüslü terim maksimum 180 derece faz değiştirebilir. QPSK için burada $M=4$ 'tür. Baz band PSK sinyalleri için kare dalga kullanılabilir. Darbe'nin genliğini "A" kabul edersek, T periyodu boyunca darbe içindeki enerji, darbe genliğinin katlarına eşit olacaktır. Eğer $R=1$ ohm alınırsa, darbe'nin enerjisi;



$$E = 1 = \frac{A^2 T}{2} \quad (8.3)$$

$$A = \sqrt{\frac{1}{T}}$$

$$p_s(t) = \sqrt{\frac{2}{T}} \quad 0 \leq t \leq T \quad (8.4)$$

Bu bağıntıyı yukarıdaki ana eşitlikte yerine koyarsak;

$$s_i(t) = A_c \sqrt{\frac{2}{T}} \cos\left(2\pi f_c t + \frac{2\pi i}{M}\right) \quad (8.5)$$

Ac'yi E cinsinden ifade edersek,

$$s_i(t) = \underbrace{\sqrt{\frac{2E_s}{T}}}_{\text{Constant}} \cos\left(\underbrace{2\pi f_c t}_{\substack{\text{Changing} \\ \text{with time}}} + \underbrace{\frac{2\pi i}{M}}_{\substack{\text{Changing} \\ \text{with info}}}\right) \quad i = 0, 1, \dots, M \quad (8.6)$$

Burada QPSK sinyali açılı bileşeni; zamanla değişen taşıyıcı frekans ve faz değişimi bileşenlerinden oluşmaktadır.

4.3.3. Raised cosine transmit filter

Bu filtre bloğu gelen sinyali yukarı frekanslara module ederek, modüleli sinyali normal cosinüs FIR filtreden geçirir. Filtrenin Karakteristiği ve filtrenin tipi, 2 tip parametre ile tayin edilir. Bunlar, normal ve kare köklü olmak üzere seçilir. Rolloff faktörü R ve sembol periyodu T olmak üzere; normal yükselen cosinüs filtresinin impulse tepkisi,

$$h(t) = 4R \frac{\cos((1+R)\pi t/T) + \frac{\sin((1-R)\pi t/T)}{(4Rt/T)}}{\pi\sqrt{T}(1-(4Rt/T)^2)} \quad (8.7)$$

Karekök artışı cosinüs filtrenin impulse cevabı ile normal artışı cosinüs filtrenin impulse cevabı birbirine eşittir. Grup gecikme parametresi, filtre tepkinin tepe değeri ile filtre tepkisinin başlangıç noktası arasındaki sembol sayısıdır. Grup gecikmesi ve yukarı örnekleme faktörü N, filtrenin tepki cevabının uzunluğunu belirler ve

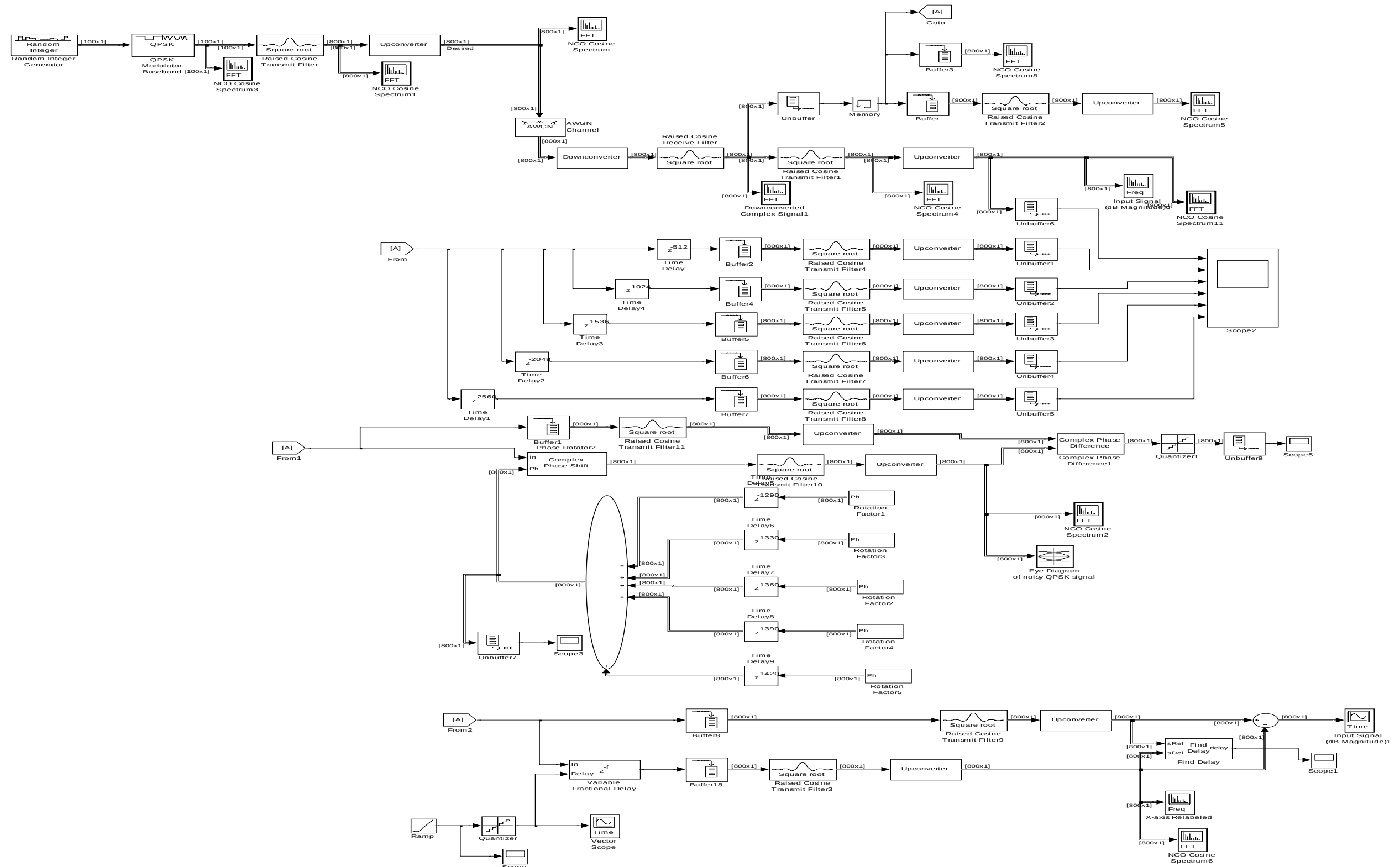
$2 \cdot N \cdot \text{Grup gecikmesi} + 1$ ile verilir. Rolloff faktörü parametresi filtrenin rolloff faktörüdür ve 0 ile 1 arasında gerçek bir sayı olmalıdır. Rolloff faktörü filtrenin band genişliğinin ne kadar aşılabileceğinin bir ölçüsüdür. Örneğin rolloff faktörü 0.5 ise bunun anlamı filtrenin band genişliği, giriş örnekleme frekansının 1.5 katıdır anlamına gelir. Filtre kazanç parametresi filtre katsayısının filtre tarafından nasıl normalize edildiğini gösterir. Eğer normalize seçeneği seçilirse, bu durumda blok otomatik ölçeklendirme kullanır. Eğer filtre tipi normal ise bu durumda filtre katsayısı tepe katsayısı 1'e eşit olacak biçimde normalize edilir. Eğer filtre tipi karekök seçilirse, bu durumda filtre katsayısı, konvolüsyonun tepe katsayısı 1 e eşit olan normal artan cosinüs filtre üretecek şekilde normalize edilir.

4.3.4. Additive White Gaussian Noise (AWGN) kanalı

AWGN kanal bloğu, giriş sinyaline beyaz Gaussian gürültü eklemek için kullanılmıştır. Eğer giriş sinyali reel ise bu blok, reel Gaussian gürültüsü ekleyerek reel çıkış sinyali üretir. Giriş sinyali karmaşık ise, bu blok karmaşık Gaussian gürültüsü ekleyerek karmaşık çıkış sinyali üretir. Bu blok giriş sinyalinden gelen örnekleme zamanını aynen kullanır.

4.4. DRFM Modellemesi ve Aldatma Karıştırması

Şekil 8.1'de simulink ile hazırlanmış olan DRFM modeli verilmiştir.

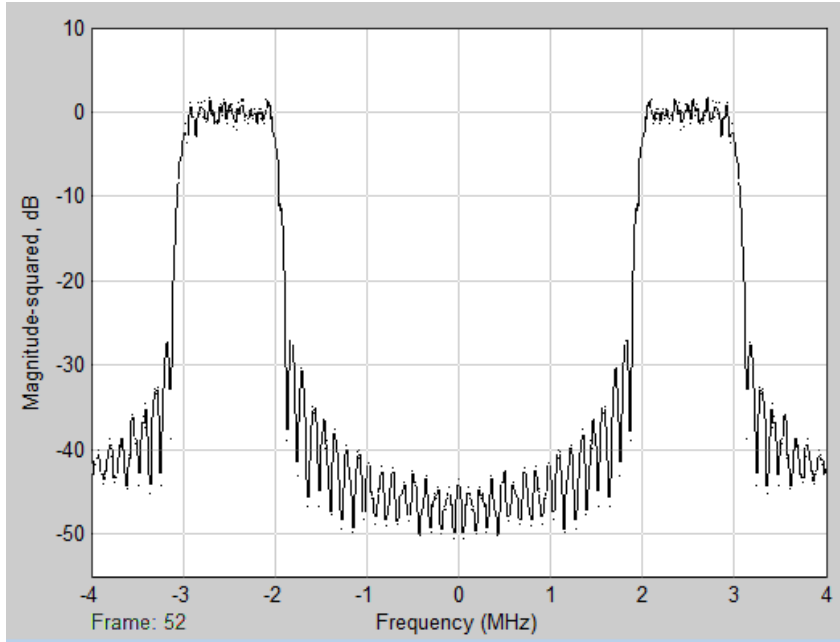


Şekil 4.3 DRFM Simulink Modeli

Hazırlanan simulink DRFM modeli aşağıdaki bölümlerden oluşmaktadır.

4.4.1. Temsili radar sinyalinin oluşturulması

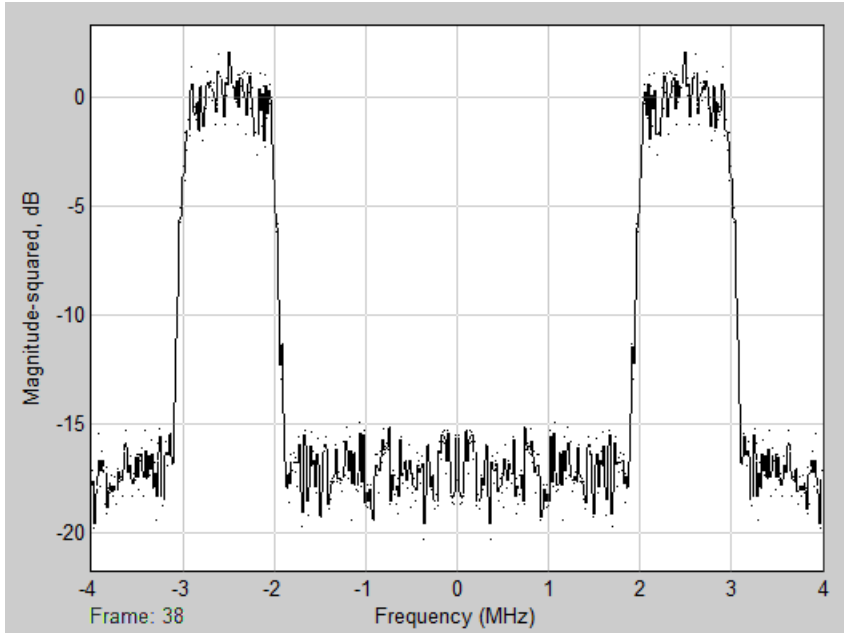
Bu bölümde DRFM girişine gelen sinyali temsil etmek üzere modüleli bir sinyal oluşturulmaya çalışılmıştır. Bu sinyalin oluşturulması için “QPSK Modulator” kullanılmıştır. QPSK modulator girişi “Random Integer Generator” ile beslenerek 4 giriş değeri için QPSK’nın 4 farklı bölgede faz kayması yaratması sağlanmıştır. Modulator çıkışındaki sinyalin darbe şeklini düzeltmek için “Raised Cosine Transmit Filter” bloğundan geçirilmiştir. Daha sonra elde edilen sinyal, yayınlanmak üzere üst frekanslara modüle edilmiştir. Modüle edilerek dış ortama yayınlanan sinyal Şekil-4.4’de gösterilmiştir.



Şekil 4.4 Temsili Radar Sinyali

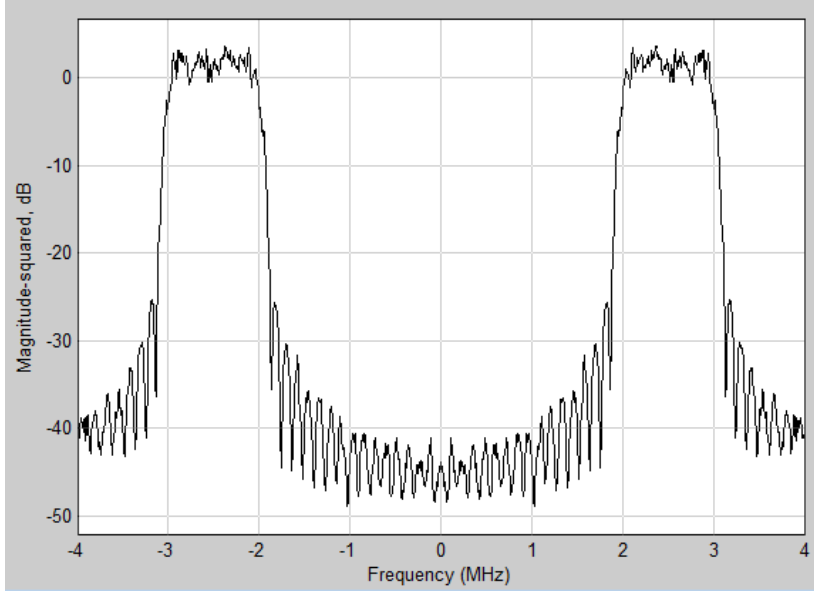
4.4.2. DRFM girişindeki sinyalin tekrar elde edilmesi

Temsili radar sinyalinin orta frekansa dönüştürülmesi ve tekrar up konvert edilerek eski sinyalin elde edilişi: 1 nolu aşamada elde edilen temsili radar sinyaline ortamdan girebilecek gürültüleri simule etmek üzere AWGN bloğu eklenmiş olup, AWGN bloğu çıkışındaki sinyal Fast Fourier Transorm (FFT) spektrumu Şekil 4.5'te gösterilmiştir.



Şekil 4.5 DRFM Girişine Gelen Sinyal

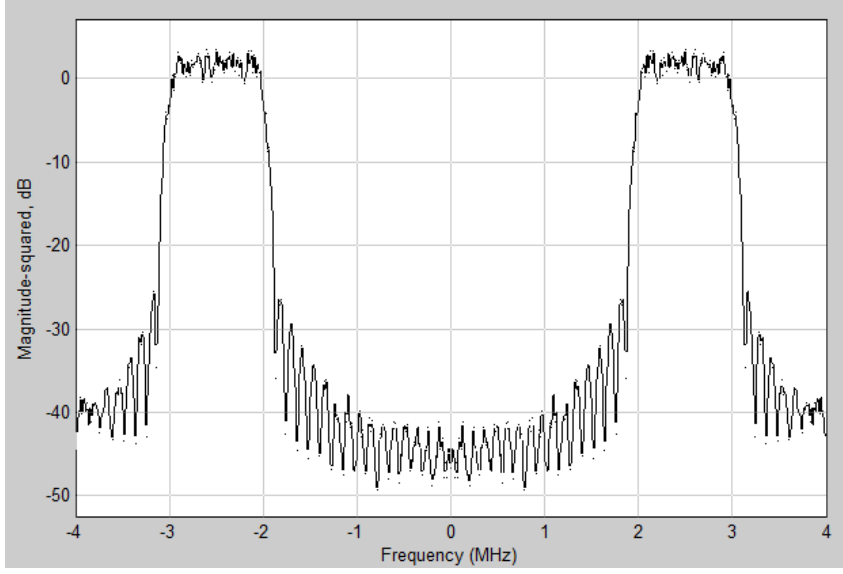
AWGN bloğundan çıkan ve DRFM girişine gelen sinyal, down converter kullanılarak IF frekansa dönüştürülmüştür. Down converter çıkışı bir alıcı filtreden geçirilmiştir. Daha sonraki karşılaştırmalarda referans olarak kullanılmak üzere DRFM girişindeki sinyali yeniden elde etmek üzere direkt bir yol oluşturulmuştur. Bu direk yolda down convert edilen sinyal transmit filtreden geçirilip, tekrar up convert edildikten sonra girişteki sinyal tekrar elde edilmiştir. Direkt yol çıkışındaki referans sinyal FFT spektrumu Şekil 4.6'da verilmiştir.



Şekil 4.6 Direkt Yol Çıkış Sinyali

4.4.3. DRFM girişindeki sinyalin kaydedilmesi

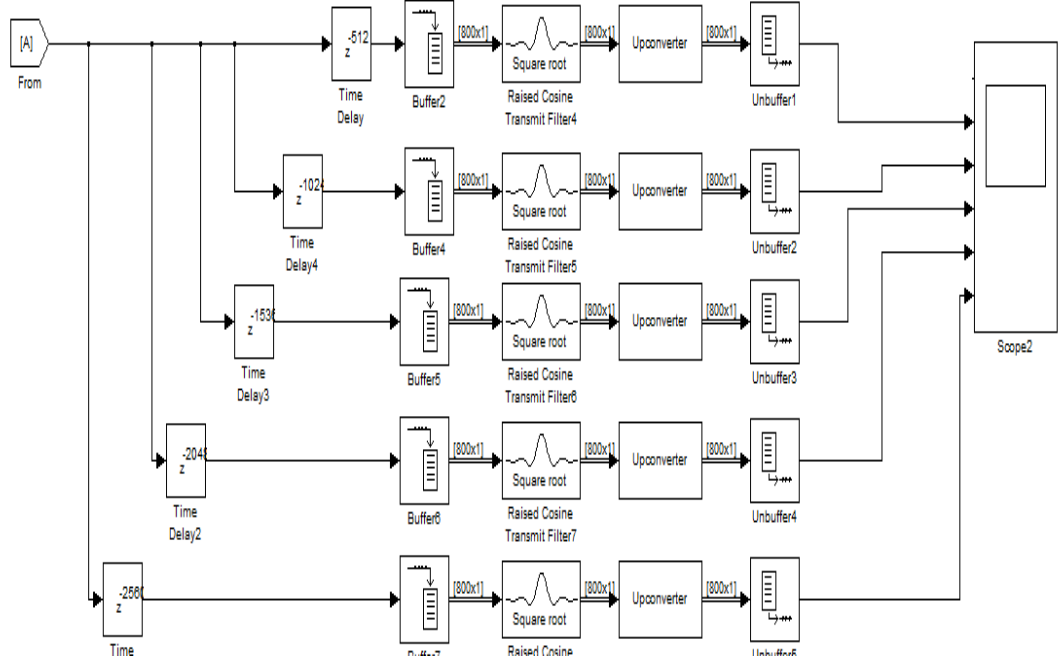
Radar sinyalinin hafızada kayıt altına alınması ve upconvert edilerek radar sinyalinin yeniden elde edilmesi: DRFM girişine gelen sinyal down convert edilip, transmit filtreden geçirildikten sonra, aldatma tekniklerinde kullanılmak üzere hafıza bloğuna kaydedilmek zorundadır. Giriş sinyalinin hafıza bloğuna kaydedilebilmesi için ayrı ayrı tamponlarda tutulan bilgilerin “unbuffer” bloğunda açılarak tekrar bir araya getirilmesi gerekmektedir. Unbuffer bloğundan geçirilen giriş sinyali hafıza bloğu tarafından kaydedilebilmektedir. Hafıza bloğunda kaydedilen bilgi daha sonra tekrar tamponlanarak transmit filtreden geçirilmekte, sonrada upconvert edilerek DRFM girişindeki sinyal tekrar elde edilmektedir. Hafızaya alınan giriş sinyalinin tekrar elde edilmiş FFT spekturum şekli, Şekil 4.7’de verilmiştir.



Şekil 4.7 DRFM’de Kaydedilen Sinyal

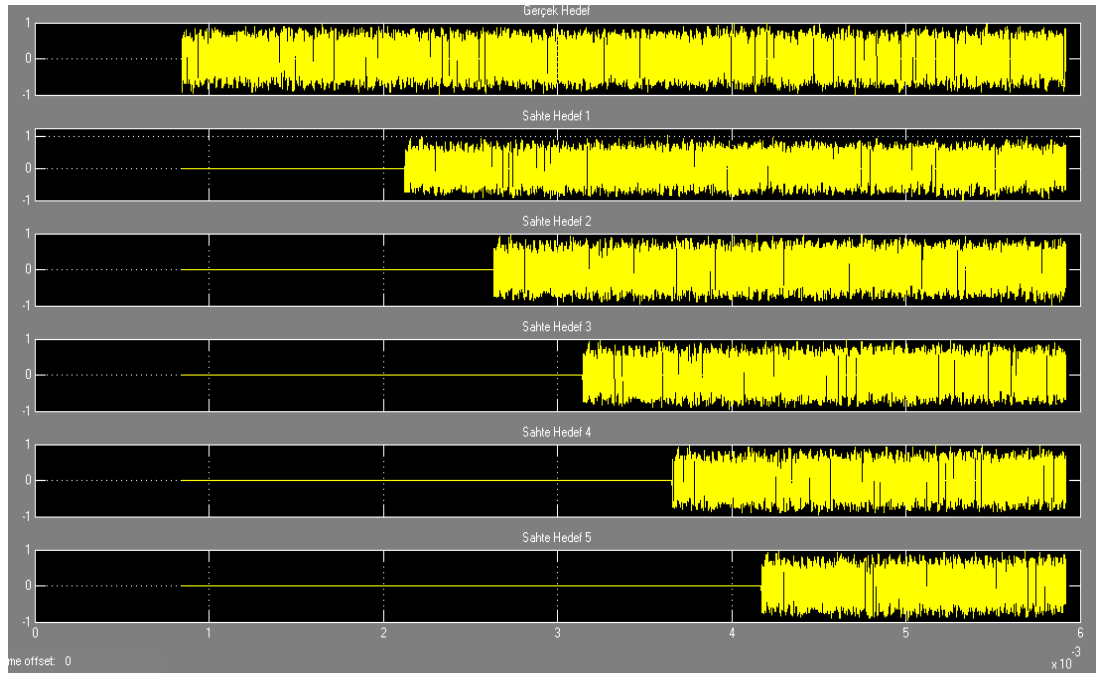
4.4.4. Farklı mesafelerde sahte çoklu hedef yaratılması

DRFM’in hafıza birimine kaydedilen giriş sinyali kullanılarak [A], eşit aralıklarla arka arkaya dizilmiş 5 adet sahte hedef yaratılmaya çalışılmış ve Şekil 4.8’de Sahte Hedef Yaratma Simulink Modeli verilmiştir.



Şekil 4.8 Sahte Hedef Yaratma Simulink Modeli

Sahte hedefler, hafızada kayıtlı sinyal birbirinden 512 örnekleme zamanı kadar geciktirmeye sahip “Time Delay” bloklarından geçirilmek suretiyle elde edilmiştir. Sahte hedefler, sırasıyla birbirlerinden 512 örnekleme zamanı kadar geride olmak üzere, birinci, ikinci, üçüncü, dördüncü ve beşinci sinyaller oluşturularak, 5 farklı sahte hedef yaratılmıştır. DRFM çıkışındaki zaman gecikmeli sinyallerin, zaman ekseninde gösterimi Şekil 4.9’da verilmiştir.

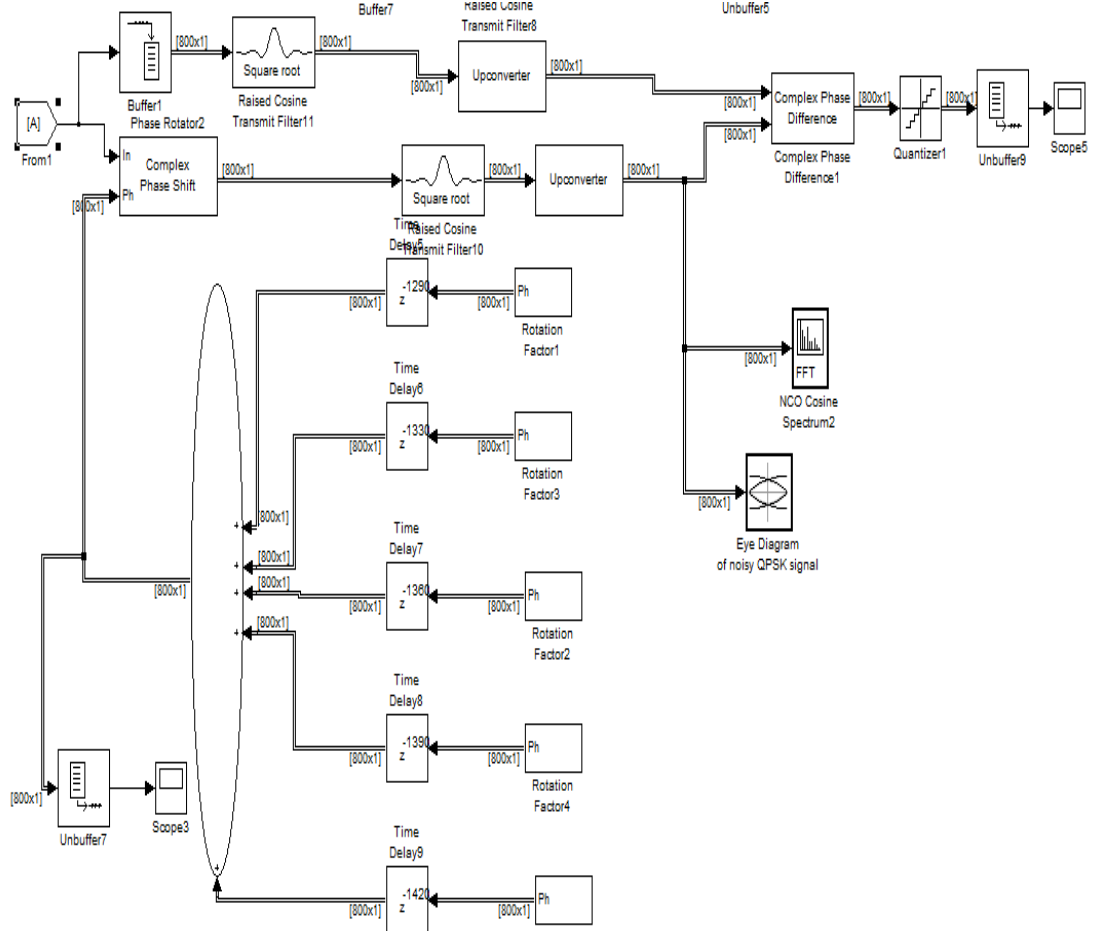


Şekil 4.9 Sahte Hedef Sinyalleri

Yukarıdaki modelle oluşturulan sinyaller bir izleme radarına kendi ekosuymuş gibi gönderilirse, izleme modundaki bu radar, bir uçağı birbirinden farklı mesafelerde yaklaşan 5 adet uçak varmış gibi görmesi sağlanacaktır.

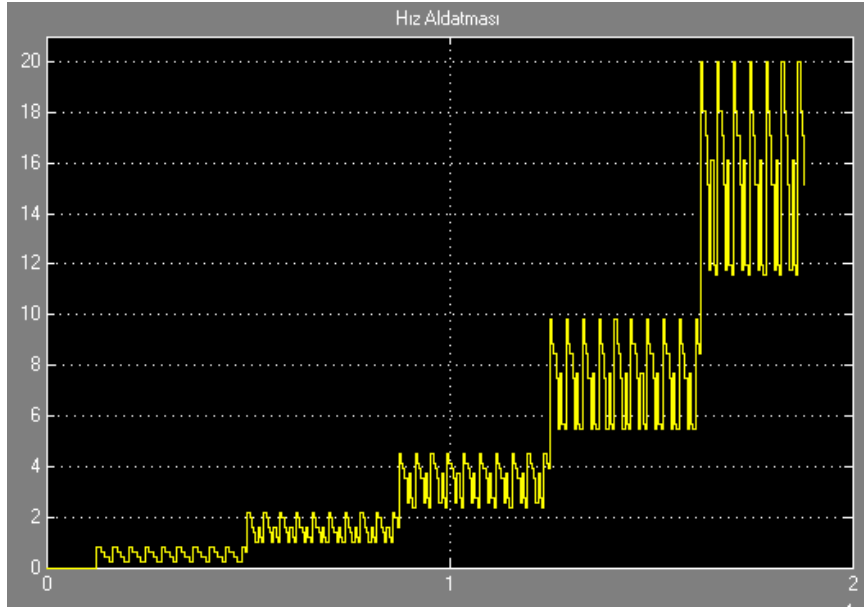
4.4.5. Hız Kapısı çalınması tekniği

VGS Simulink Modeli Şekil 4.10’da verilmiştir.



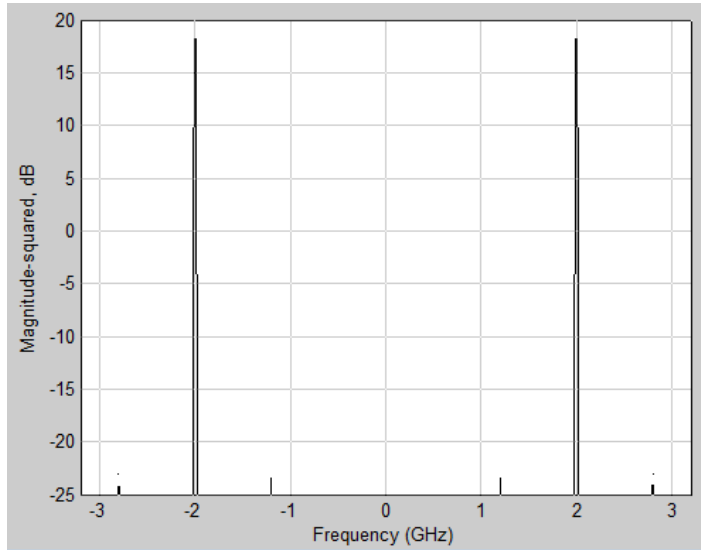
Şekil 4.10 VGS Simulink Modeli

Radarın hız kapısının çalınabilmesi için öncelikle, zaman içinde radara geri dönen ekolarda meydana gelen doppler kayması kadar kaymaya sahip ve onlardan daha büyük genlikte sinyallerin oluşturulması gerekmektedir. Daha sonra doppler kayması yavaş yavaş artırılarak, radarın hız kapısına, üretilen sahte sinyalin oturtulması sağlanacaktır. Sahte doppler kaymasının oluşturulması için “Complex Phase Shift - CPS” bloğundan yararlanılmıştır. Radarın hız kapısının çekildiğini fark etmemesi için CPS girişine, birbirinden farklı değerlere sahip 5 ayrı sinyal toplanarak uygulanmış ve bu sinyal Şekil 8.9’da verilmiştir. CPS tarafından ise girişine uygulanan sinyale bağlı olarak faz farkı oluşturulmuştur.



Şekil 4.11 CPS Girişindeki Sinyal

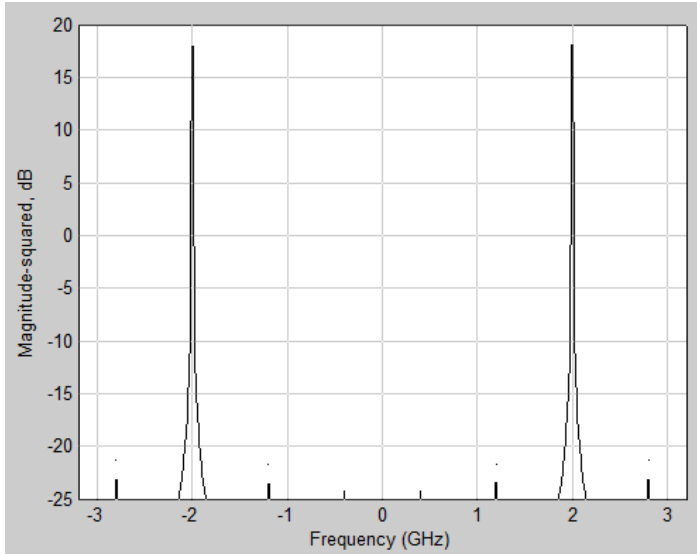
Faz farkı yaratılmadan önce CPS yolu (Path) sonunda FFT spekturum şekli Şekil 4.12’de gösterilmiştir.



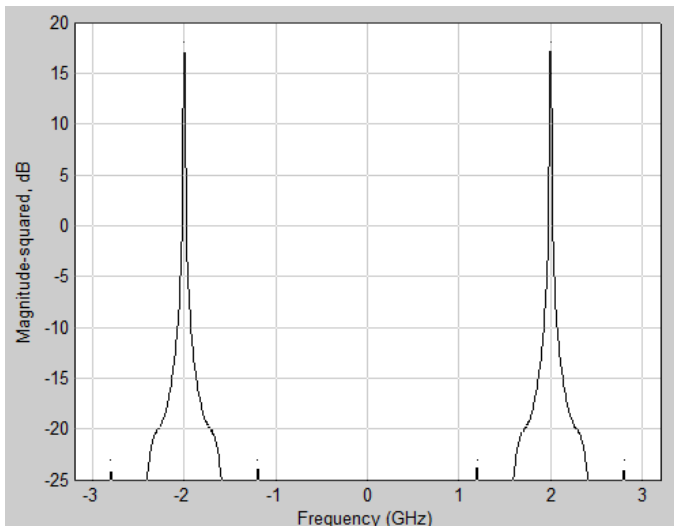
Şekil 4.12 Faz Farkı Yaratılmadan Önceki Sinyal

CPS tarafından faz farkı yaratıldıktan sonra, 5 farklı sinyal belirli bir gecikme ile sırasıyla uygulandığından, DRFM çıkışındaki FFT sinyal spektrumunda, fazın yavaş

yavaş deđiřtiđi anlařılmakta olup, elde edilen spektrumlar zaman sıralamalı olarak řekil 4.13.a, b, c’de verilmiřtir.



(a)



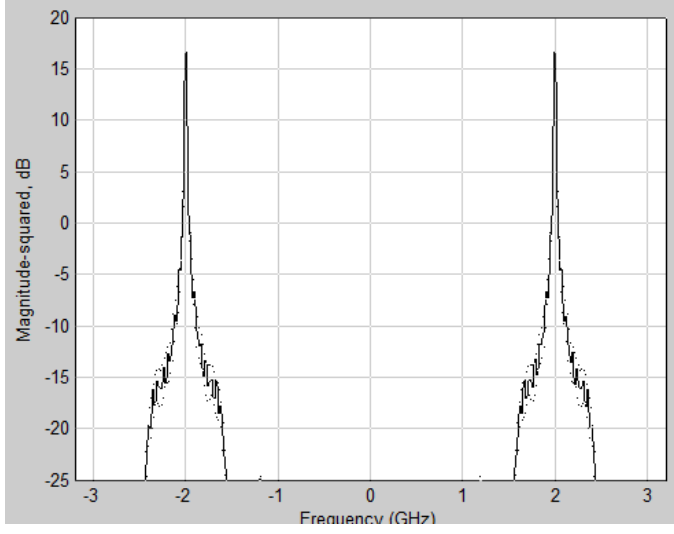
(b)

řekil 4.13. VGS Sinyali (a) VGS Sinyali-1 (b)

VGS

Sinyali-2

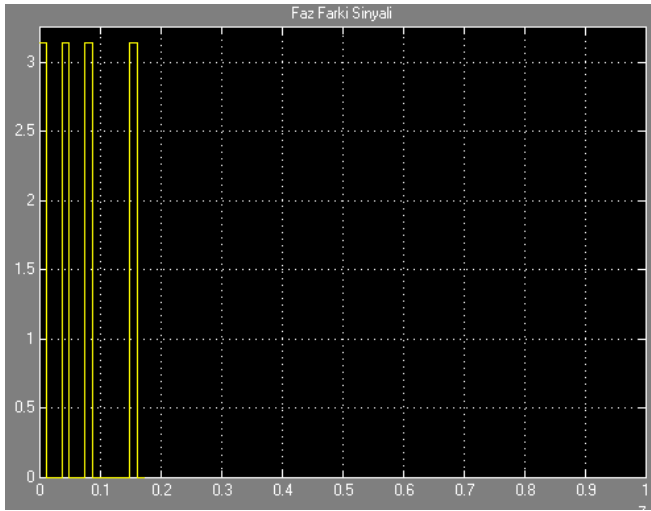
(c) VGS Sinyali-3



(c)

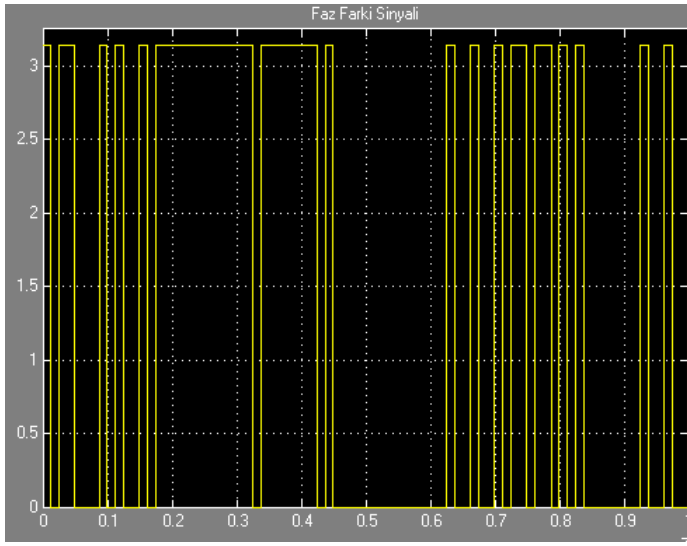
Şekil 4.13. (Devam) VGS Sinyali (a) VGS Sinyali-1 (b) VGS Sinyali-2
(c) VGS Sinyali-3

Çıkıştaki faz farkının daha iyi anlaşılabilmesi amacıyla, VGS Simulink modeli çıkışına “Complex Phase Difference –CPD” bloğu konulmuştur. Bu blok sayesinde [A] sinyali ile faz kaydırılmış sinyal arasındaki farkın alınması sağlanmıştır. CPD çıkışından elde edilen sinyaller Şekil 8.12.a, b, c’de verilmiştir.

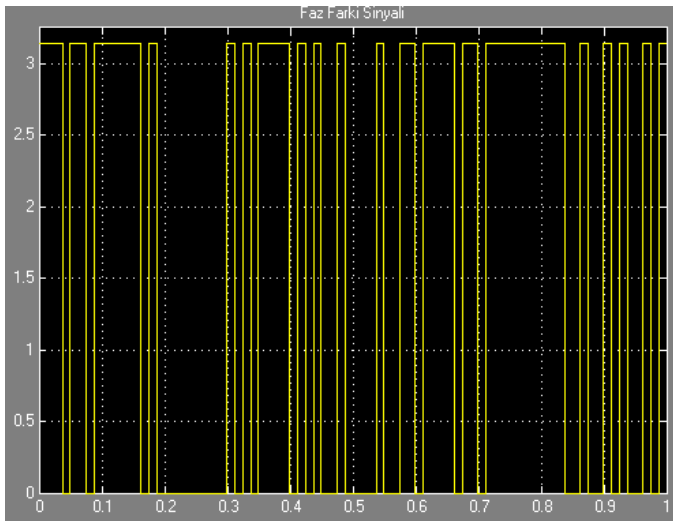


(a)

Şekil 4.14. CPD Çıkışı Sinyali (a) CPD Çıkışı Sinyali-1 (b) CPD Çıkışı Sinyali-2 (c) CPD Çıkışı Sinyali-3



(b)

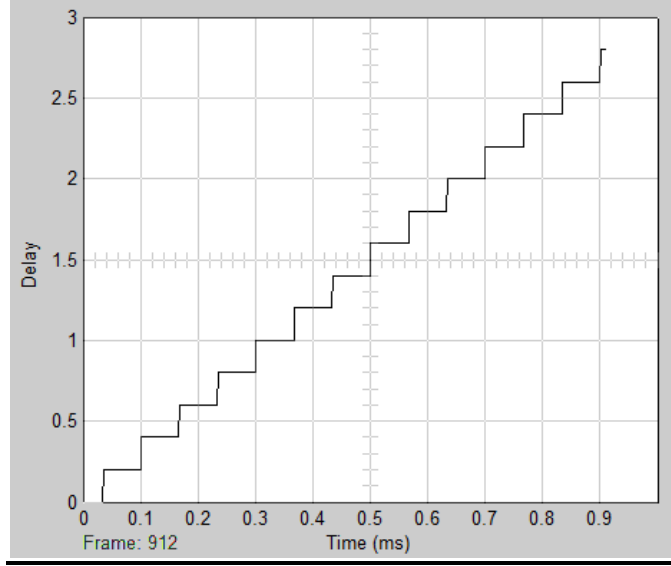


(c)

Şekil 4.14. (Devam) CPD Çıkışı Sinyali (a) CPD Çıkışı Sinyali-1 (b) CPD Çıkışı Sinyali-2 (c) CPD Çıkışı Sinyali-3

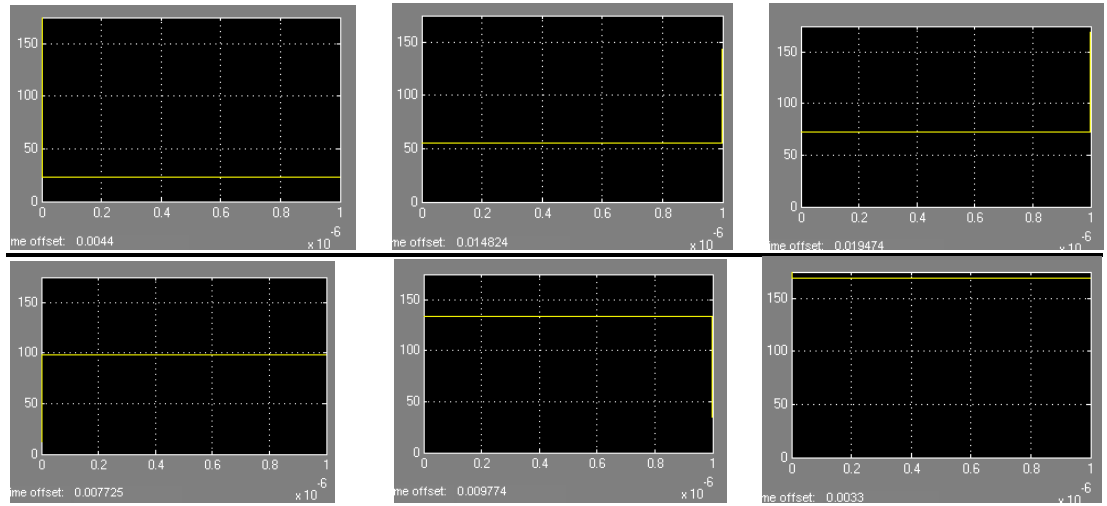
Yukarıdaki modelle oluşturulan sinyaller bir izleme radarına kendi ekosuymuş gibi gönderilirse, izleme radarı uçağı olduğundan daha hızlı kendisine yaklaşıyormuş izlenimi edinecektir.

üzere “Quantizier” (Dilimleme aralığı 0,0001) bloğundan geçirilmiş ve çıkışı Şekil 4.16’da verilmiştir.



Şekil 4.16 Lineer RGS Sinyali

RGS’nin çıkış spektrumunu gösterebilmek için “Find Delay-FD” bloğu kullanılmıştır. FD girişlerine memory çıkışı ve VFD çıkışı bağlanarak, iki sinyal arasındaki gecikme farkı ölçülmüş ve Şekil 4.17’de verilmiştir.



Şekil 4.17 RGS Fark Gecikme Sinyali

Yukarıdaki Şekilde FD çıkışının zamanla arttığı görülmektedir. Bu şekilde zamanla artıp, azalan bir gecikme yapılabilmesi radarın mesafe kapısının çalınabileceğini göstermektedir.

Yukarıdaki modelle oluşturulan sinyaller bir izleme radarına kendi ekosuymuş gibi gönderilirse, izleme radarının mesafe kapısı çalınarak, kendisine doğru yaklaşan bir uçağı uzaklaşıyormuş gibi algılayacaktır.

5. SONUÇ VE ÖNERİLER

Bu çalışmada, çağımızda ülkelerin savunmasında vazgeçilmez bir unsur olarak gündemde kalacak olan elektronik harp ve elektronik taarruzun bir bölümü olan elektronik aldatma teknikleri incelenmiştir. Elektronik harbin, hava platformları ile ilgili alanları üzerinde durulmuştur.

Bu çalışmada, MatLab Simulink programı kullanılarak DRFM modellenmiştir. Bu modelde, aldatma karıştırmasına maruz kalacak radar sinyalinin temsil etmek üzere, QPSK modülasyonu kullanılarak temsili bir radar sinyali oluşturulmuştur. Bu sinyale, sinyal boşlukta yayılırken ortamdan girebilecek gürültüler de dikkate alınarak gürültü eklenmiş, DRFM girişine ulaşan bu sinyal down convert edilerek IF'ye düşürülmüştür. IF frekansa indirilen sinyal, filtreden geçirilmek suretiyle hafıza bloğunda kayıt edilmiştir. Kayıt işlemi gerçekleştirilen sinyal hafızadan çağrılarak, karıştırma tekniklerinden; çoklu sahte hedef yaratma, RGPO ve VGPO olmak üzere 3 farklı karıştırma tekniği uygulanmıştır. Bu tekniklerden çoklu sahte hedef yaratma uygulamasında, hafızada kayıtlı sinyal gecikme bloklarından geçirilerek, izleme modundaki radara, bir uçak birbirinden farklı mesafelerde ilerleyen 5 adet uçak varmış gibi gösterilmiştir. VGPO uygulamasında, hafızada kayıtlı sinyale karmaşık faz kayması eklenerek yavaş yavaş artan doppler faz kayması uygulanmış ve hız kapısı çalınmıştır. Böylece uçak olduğundan daha hızlı hedefe yaklaşıyormuş izlenimi verdirilmiştir. RGPO uygulamasında ise, kayıtlı sinyale zamanla lineer artan gecikme sinyali uygulanarak radarın mesafe kapısı çalınmış ve radara doğru yaklaşan bir uçağın, radar tarafından uzaklaşıyormuş gibi algılanması sağlanmıştır.

Bu çalışmada geliştirilen DRFM modeli kullanılarak ve bu model girişine sayısal kanal alıcı bloğu eklenerek, daha hızlı ve daha geniş bantta çalışan bir DRFM elde edilebilir. Böylece büyük kapasiteli hafıza birimlerine ihtiyaç duyulmadan, değişik radar sinyallerine hızlı bir şekilde gerçek zamanlı karıştırma uygulanabilir. Ayrıca bu modelde kullanılan QPSK modülasyonu yerine, değişik tipte modülasyonlar kullanılarak, karıştırma tekniklerinin etkinliği araştırılabilir. Modelden elde edilen çıkış sinyallerinde, örnekleme ve dilimleme sırasında oluşan istenmeyen gürültü ve

sahte sinyaller incelenerek, DRFM ile üretilmiş aldatma sinyalinin gerçek sinyalden ayırt edilebilmesi konusunda çalışmalar yapılabilir. Günümüzde elektronik harbin bir gereği olarak, DRFM'lerin kullanılması ile birlikte radarlara, DRFM'ler tarafından istenilmeden üretilen gürültüleri algılayarak, kendi ekosunu karıştırma sinyalinden ayırt ettirme imkanı sağlayacak kabiliyetler kazandırılmaya çalışılmaktadır.

DRFM teknolojisi, geniş bandlarda kayıt yapabilmeleri nedeni ile, bilinmeyen bölgelerdeki sinyallerin kaydedilerek istihbarat amaçlı kullanılmasına imkan sağlayabilir. Kaydedilen sinyaller anlık ya da daha sonra kayıttan ayrıntılı olarak incelenebilir. Ayrıca DRFM'ler ile çeşitli özelliklerde sinyaller üretilerek, radar sinyal simulatörü olarak kullanılabilir.

Elimizde en son teknolojiye sahip RF tabanlı sistemleri olan gelişmiş bir helikopter olsa bile, IR güdümlü omuzdan atılan bir füze ile helikopterinizi düşürülebilir ve RF sistemler bir işe yaramayabilir. Bu nedenle, ülkeler bu alanda araştırma geliştirme projelerine daha fazla ağırlık vermelidir. Hangi tabanlı olursa olsun savunma sistemlerinin güvenilir olabilmesi için tamamen milli olarak üretilmeleri şarttır. Bu nedenle üniversitelerimizde sürdürülen Ar-Ge projeleri desteklenmeli, üniversitelerde geliştirilen teknolojilerin, savunma sanayinde kullanılabilecek sistemler haline dönüştürülebilmesi için yerli savunma sanayi şirketleri teşvik edilmelidir.

KAYNAKLAR

1. Neri, F., "Introduction to Electronic Defense Systems 2nd ed", **Artech House**, 374-462 (1991).
2. Schlesinger, R. J., "Principle of Electronic Warfare", **Peninsula Publishing**, California, 154-170 (1961)
3. NITYANANDA B.V., "Spurs in Digital Radio Frequency Memory and Applications of DRFM", Yüksek Lisans Tezi, **Naval Postgraduate Scholl**, Monterey CA, 5-14 (1993)
4. Skolnik M.I., "Introduction to Radar Systems" **McGraw-Hill**, 152-186 (1980)
5. Van Brunt L. B., "Applied ECM, 1st. EW ed", **Artech House**, 321-356 (1982)
6. Kural F., Özkazanç Y., "A Method For Detecting RGPO/VGPO Jamming", **Signal Processing and Communications Applications Conference, 2004 Proceedings of the IEEE 12th**, 237-240 (2004)
7. Schleher D.C., "Introduction to Electronic Warfare", **Artec House**, Norwood, 109-183 (1993)
8. Adamy D., "EW 101:A First Course in Electronic Warfare", **Artec House**, 177-219 (2002)
9. Kwak, C.M., "Application of DRFM in ECM for pulse type radar" , **Infrared, Millimeter, and Terahertz Waves, 2009. IRMMW-THz 2009. 34th International Conference on 21-25 Sept. 2009**, 1-2 (2009)
6. Zongbo Wang, Meiguo Gao, Yunjie Li, Haiqing Jiang, Sunguo Ying, "The Hardware Platform Design for DRFM System", **Signal Processing, 2008. ICSP 2008. 9th International Conference on 26-29 Oct. 2008**, 426-430 (2008)
7. Berger, S.D., "The Spectrum of a Digital Radio Frequency Memory Linear Range Gate Stealer Electronic Attack Signal", **Radar Conference, 2001. Proceedings of the 2001 IEEE**, 27-30 (2001)
8. Berger, S.D., "Digital Radio Frequency Memory Linear Range Gate Stealer Spectrum", **Aerospace and Electronic Systems, IEEE Transactions on** 39(2): 725-735 (2003)

9. Berger, S.D.; Meer, D.E., “An Expression for the frequency Spectrum of a Digital Radio Frequency Memory Signal”, **Aerospace and Electronics Conference, 1990. NAECON 1990., Proceedings of the IEEE 1990 National**, 90-93 (1990)
10. Pring, P.C.J.; James, G.E.; Hayes, D.; White, M.P., “The Phase Performance Of Digital Radio Frequency Memories (DRFMs)”, **Advanced A-D and D-A Conversion Techniques and their Applications, 1994. Second International Conference on 6-8 Jul 1994**, 18-23 (1994)
11. E.J.Chrzanowski, “Active Radar Electronic Counter Measures”, **Artech House**, 51-162 (1990)
12. Townsend, J.D.; Saville, M.A.; Hongy, S.M.; Martin, R.K., “Simulator for Velocity Gate Pull-Off electronic countermeasure techniques”, **Radar Conference, 2008. RADAR '08. IEEE**, 1-6 (2008)
13. Güvenç, M.M., “Uçaklardaki Darbeli Doppler Radarları İçin Elekktronik Karıştırmanın Algılama Menziline Etkisi”, Yüksek Lisans Tezi, **İTÜ Fen Bilimleri Enstitüsü**, İstanbul, 55-64 (2002)

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : DİNÇ, Veysel
 Uyuğu : T.C.
 Doğum tarihi ve yeri : 01.12.1972 Ankara
 Medeni Hali : Evli
 Telefon : 0 536 237 70 95
 e-mail : vysl_dinc@hotmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Lisans	Gazi Üniv. Elek.Elektronik Müh.Böl.	1995
Lise	Yenimahalle Teknik Lisesi	1990

İş Deneyimi

Yıl	Yer	Görev
1996-1998	Gantek A.Ş.	Sist.Destek Müh.
1998-2010	Hv.K.K.lığı	EH TYS Müh.

Yabancı Dil

İngilizce

Hobiler

Araba kullanmak, Müzik dinlemek.