
GAZİ ÜNİVERSİTESİ
Gazi
1926

# HAVA ARAÇLARININ ADS-B SİNYALLERİ YARDIMIYLA SINIFLANDIRILMASI

**Gürsu GÜRER**

**YÜKSEK LİSANS TEZİ**
**ELEKTRİK - ELEKTRONİK MÜHENDİSLİĞİ ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**NİSAN 2024**

## ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Gürsu GÜRER

26/04/2024

# HAVA ARAÇLARININ ADS-B SİNYALLERİ YARDIMIYLA SINIFLANDIRILMASI

(Yüksek Lisans Tezi)

Gürsu GÜRER

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Nisan 2024

## ÖZET

Hava trafik yoğunluğunun günden güne artması ve bu trafiğin yönetilebilmesi amacıyla giderek daha fazla öneme sahip olan Otomatik Bağımlı Gözetim-Yayın (ADS-B) sistemleri, herhangi bir yer/hava kullanıcısının ihtiyaç duyacağı pozisyon, iz ve yer hızı vb. bilgilerin bir yayın kaynağı aracılığıyla belli aralıklarla iletimini sağlayan bir gözetim uygulamasıdır. ADS-B out ve ADS-B in olarak 2 farklı servisi olan ADS-B, radar sisteminin yerini alarak tüm dünyada hava trafiğini yönetme yolundadır. ADS-B protokolünde yayınlanan mesajlar kriptolu (encrypted) ya da yetkilendirilme anahtarına sahip (authenticated) değildir. Bu sebeple bir çeşit SDR (Software Define Radio) ya da benzeri düşük bütçeli cihaz ile bu yayınlar kolayca dinlenebilir ya da sahte ADS-B mesajları yayınlanarak siber saldırılar gerçekleştirilebilir. Bu tarz saldırıların önüne geçilmesi için Radyo Frekans Parmak izi (RFF), sinyallerin sınıflandırılması için başarılı sonuçlar üretebilir. Bu çalışmada, hava araçlarının kimliklendirilebilmesi için ADS-B yayın kaynakları RFF vasıtasıyla sınıflandırılmıştır. SDR yardımıyla 8 farklı uçaktan 3480 adet gerçek ADS-B sinyali kaydedilmiştir. Bu sinyallerin benzersiz parmak izinin çıkartılması için güç spektral yoğunluğu (PSD) özelliği kullanılmıştır. Doğrusal, polinom ve dairesel tabanlı (RBF) kernel fonksiyonu ile destek vektör makinaları kullanarak hava araçları kimliklendirilmiştir. Kimliklendirme esnasında farklı sinyal-gürültü oranlarına (SNR) göre test sonuçları gözlemlenmiştir. En düşük SNR seviyesinde (10 dB) dahi önerilen SVM metodunda polinom kernel fonksiyonu kullanarak %92'lik bir başarım yakalanmıştır. Az sayıda ve düşük SNR'a sahip gerçek sinyallerden oluşan veri setiyle dahi RFF sınıflandırmasının başarılı olabileceğini gösterilmiştir.

Bilim Kodu : 90541

Anahtar Kelimeler : Yapay zekâ, makine öğrenmesi, ADS-B, RFF, SVM

Sayfa Adedi : 59

Danışman : Prof. Dr. Ali KARA

CLASSIFICATION OF AIRCRAFTS BY MEANS ADS-B SIGNALS

(M. Sc. Thesis)

Gürsu GÜRER

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

April 2024

## ABSTRACT

The increasing daily air traffic density and the necessity to manage this traffic have elevated the importance and usage of Automatic Dependent Surveillance-Broadcast (ADS-B) systems. These systems serve as a surveillance application that broadcasts essential information such as position, track, and ground speed at regular intervals through a broadcast source to any terrestrial or aerial user requiring it. ADS-B, with its two distinct services, ADS-B Out and ADS-B In, is on the path to replace radar systems, managing air traffic worldwide. The messages broadcasted by the ADS-B protocol are neither encrypted nor authenticated. Therefore, these broadcasts can be easily intercepted or spoofed with fake ADS-B messages using a Software Defined Radio (SDR) or similar low-cost devices, leading to potential cyber-attacks. Radio Frequency Fingerprinting (RFF) of signals for classification can produce successful results in preventing such attacks. In this study, ADS-B broadcast sources were classified to identify aircraft. With the assistance of SDR, 3480 real ADS-B signals from 8 different aircraft were recorded. The Power Spectral Density (PSD) feature was utilized to extract the unique fingerprint of these signals. Air vehicles were identified using Support Vector Machines (SVMs) with linear, polynomial, and Radial Basis Function (RBF) kernel functions. The test results were observed across different Signal-to-Noise Ratios (SNRs). At the lowest SNR level (10 dB), the proposed SVM method using the polynomial kernel function achieved a success rate of 92%. This demonstrates that RFF classification can be successful even with a small dataset consisting of real signals at low SNRs.

Science Code : 90541
Key Words : Artificial intelligence, Machine learning, ADS-B, RFF, SVM
Page Number : 59
Supervisor : Prof. Dr. Ali KARA

# TEŞEKKÜR

Bu tez çalışmasının her aşamasında engin bilgi birikimi ve tecrübesi ile bana yol gösteren, her konuda yanımda olan, kendisiyle çalışmaktan onur durduğum çok değerli danışman hocam Prof. Dr. Ali KARA'ya en içten saygı ve teşekkürlerimi sunarım.

Çalışmama sağlamış olduğu katkılarından ve kıymetli desteklerinden dolayı değerli jüri üyesi hocam Doç. Dr. Yaser DALVEREN'e saygı ve teşekkürlerimi borç bilirim. Çalışmamın değerlendirilmesindeki titiz ve yapıcı yaklaşımından dolayı değerli jüri üyesi hocam Dr. Öğr. Üyesi Funda ERGÜN YARDIM'a içten teşekkürlerimi sunarım.

Bana her zaman güvenen ve her koşulda destekleyen canım fedakar ailem ile minik tatlı yeğenim Göksu GÜRER'e minnet dolu teşekkürlerimi sunarım.

Son olarak, can yoldaşım, çok değerli eşim Özge GÜRER'e ve hayatımın anlamı canım oğlum Özgür GÜRER'e en derin duygularımla teşekkür ederim.

# İÇİNDEKİLER

**Sayfa**

ÖZET ..... iv

ABSTRACT ..... v

TEŞEKKÜR ..... vi

İÇİNDEKİLER ..... vii

ŞEKİLLER LİSTESİ ..... x

ÇİZELGELER LİSTESİ ..... xi

SİMGELER VE KISALTMALAR ..... xii

1. GİRİŞ ..... 1

2. ADS-B TEKNOLOJİSİ VE GÜVENLİ HABERLEŞME ..... 3

2.1. ADS-B Teknolojisi ..... 3

2.1.1. ADS-B sistemi ve genel tasarımı ..... 4

2.1.2. ADS-B yayın sıklığı ..... 6

2.1.3. ADS-B 1090ES mesaj formatı ..... 6

2.1.4. Kapasite ..... 7

2.1.5. ICAO Kodu ..... 8

2.1.6. ADS-B mesaj tip kodları ..... 9

2.1.7. ADS-B uçak kimliği paketi ..... 9

2.1.8. Seyir konumu ..... 11

2.1.9. Yeryüzündeki konum ..... 12

2.1.10. Seyir hızı ..... 13

2.1.11. Uçağın operasyonel durumu ..... 14

2.1.12. ADS-B hata kontrolü ..... 14

2.1.13. Mesaj çözümleme örneği ..... 14

2.2. ADS-B Güvenlik Sorunları ..... 15

**Sayfa**

2.2.1. Kolay dinlenebilme (eavesdropping) ..... 17
2.2.2. Mesaj yerleştirme (message injection) ..... 18
2.2.3. Mesaj silme (message deletion) ..... 18
2.2.4. Mesaj modifiye etme (message modification) ..... 19
2.2.5. Karıştırma (jamming) ..... 19
2.3. ADS-B Güvenliği Sağlama Methodları ..... 20
2.3.1. Kriptolama yöntemleri ..... 20
2.3.2. Kalman Filtrelemesi ..... 22
2.3.3. Yayılı Spektrum (Spread Spectrum) ..... 22
2.3.4. Mesafe Sınırlayıcı (Distance Bounding) ..... 23
2.3.5. Radyo Frekans Parmak İzi (RFF) ..... 23
2.4. ADS-B Güvenliği Hakkında Literatürdeki Çalışmalar ..... 23
3. RADYO FREKANS PARMAK İZİ ..... 25
3.1. Benzersiz özellik çıkarımı (feature extractions) ..... 26
3.1.1. Geçici durum temelli özellikler (transient based features) ..... 26
3.1.2. Kararlı durum temelli özellikler (steady-state based features) ..... 26
3.1.3. Zaman-frekans analizi ..... 26
3.1.4. Modülasyon tabanlı özellikler ..... 27
3.2. I/Q Verisi ..... 27
3.3. Literatürde ADS-B ile RFF Çalışmaları ..... 28
4. VERİ TOPLAMA VE FİLTRELEME ..... 31
4.1. Verilerin Toplanması ..... 32
4.2. Temel Filtreleme Yöntemleri ..... 33
4.2.1. Alçak Geçiren Filtre ..... 33
4.2.2. Yüksek Geçiren Filtre ..... 34
4.2.3. Bant Geçiren Filtre ..... 34

**Sayfa**

4.2.4. Hareketli Ortalama Filtre ..... 34
4.3. Normalizasyon İşlemleri ..... 36
4.4. ADS-B Sinyal Özelliği Çıkarımı ..... 38
5. SINIFLANDIRMA ÇALIŞMALARI ..... 41
5.1. Destek Vektör Makinaları (SVM) ..... 41
5.2. Veri Setleri Oluşturulması ve Gürültü Eklenmesi ..... 44
5.2.1. Sinyal/gürültü oranı hesaplanması ..... 44
5.2.2. Gürültü eklenmesi ..... 46
5.3. SVM Sınıflandırması ..... 46
5.4. Sınıflandırma Sonuçları ..... 48
6. TARTIŞMA VE SONUÇ ..... 51
6.1. Tartışma ..... 51
6.2. Sonuç ..... 52
KAYNAKLAR ..... 55
ÖZGEÇMİŞ ..... 59

# ŞEKİLLER LİSTESİ

**Şekil** **Sayfa**

Şekil 2.1. ADS-B sisteminin ana bileşenleri ve sistem akışı ..... 4

Şekil 2.2. 1090ES data link formatı ..... 7

Şekil 2.3. Canlı olarak konum, hız, yükseklik vb. verilerin takip edilebildiiği FlightRadar uygulaması görseli ..... 17

Şekil 3.1. Direkt-dönüşüm mimarisiyle tipik SDR örneği ..... 27

Şekil 4.1. ADS-B Sinyali kayıt aşamaları ..... 31

Şekil 4.2. MATLAB'da SDR ile gerçek zamanlı ADS-B mesajları takip uygulamasına ait arayüz ..... 31

Şekil 4.3. Sinyal kaydının gerçekleştiği alan ..... 32

Şekil 4.4 (a) Filtreleme öncesi kayıt edilmiş örnek ADS-B sinyali; (b) Filtreleme sonrası örnek sinyal ..... 35

Şekil 5.1. Üçgen ve daire örneklerini (verileri) en yüksek marj ile optimal bir hiper düzlem kullanarak ayırma. Hiper düzleme en yakın olan destek vektörleri, dolu üçgenler ve daireler ile gösterilmiştir. ..... 42

Şekil 5.2. Tipik bir ADS-B sinyalindeki "sinyal" ve "gürültü" bölgeleri ..... 45

Şekil 5.3. SNR oranı düşük, gürültü eklenmiş ADS-B sinyali ..... 46

Şekil 5.4. Toplam 8 uçak için SVM sınıflandırmasında kullanılan örnek model ..... 47

Şekil 6.1. SVM sınıflandırmasının kernel fonksiyonlarına göre sonuçları ..... 53

# ÇİZELGELER LİSTESİ

**Çizelge** **Sayfa**

Çizelge 2.1. ADS-B mesajlarının güncellenme sıklığı ..... 6

Çizelge 2.2. 1090ES Mesaj İçeriği ..... 7

Çizelge 2.3. Kapasite değerleri karşılıkları ..... 8

Çizelge 2.4. ADS-B Mesajlarının Tip Kodları ve İçerikleri ..... 9

Çizelge 2.5. ADS-B uçak kimliği mesaj paketinin içerik dağılımı ..... 9

Çizelge 2.6. Karakter çözümlemesi için gerekli çevrim tablosu ..... 10

Çizelge 2.7. Tip Kodu ve Kapasitenin birlikte karşılıkları ..... 10

Çizelge 2.8. Havadaki konum mesaj paketinin içerik dağılımı ..... 11

Çizelge 2.9. Havadaki konum mesaj paketinin yapısı ..... 11

Çizelge 2.10. Yerdeki konum mesaj paketinin içerik dağılımı ..... 12

Çizelge 2.11. Yerdeki konum mesaj paketinin yapısı ..... 12

Çizelge 2.12. Havadaki hız mesaj paketinin yapısı ..... 13

Çizelge 2.13. Ham verinin (HEX) Çözümlenmesi ..... 15

Çizelge 2.14. Mesaj kısmının çözümlenmesi ..... 15

Çizelge 2.15. ADS-B saldırılarındaki risk analizi ..... 16

Çizelge 3.1. Literatürde bulunan RFF ile ADS-B sinyallerini sınıflandıran çalışmalar. 30

Çizelge 5.1. Tüm SVM sınıflandırmaları için kullanılan parametreler ..... 47

Çizelge 5.2. Farklı SNR değerlerinde gerçekleştirilen polinom kernel fonksiyonlu SVM sınıflandırma (%) sonuçları ..... 49

Çizelge 5.3. Farklı SNR değerlerinde gerçekleştirilen polinom kernel fonksiyonlu SVM sınıflandırma (%) sonuçları ..... 50

Çizelge 5.4. Farklı SNR değerlerinde gerçekleştirilen RBF kernel fonksiyonlu SVM sınıflandırma (%) sonuçları ..... 50

# SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

| **Simgeler** | **Açıklamalar** |
|---|---|
| **mhz** | Megahertz |
| **db** | Desibel |
| **hz** | Hertz |

| **Kısaltmalar** | **Açıklamalar** |
|---|---|
| **ACAS** | Hava Çarpışma Önleme Sistemi |
| **ADS-B** | Otomatik Bağımlı Gözetim-Yayın |
| **ANN** | Yapay Sinir Ağı |
| **ASCII** | Bilgi değişimi için Amerikan standart kodu |
| **ATC** | Hava Trafik Kontrol |
| **ATM** | Hava Trafik Yönetimi |
| **ATSP** | Hava Trafik Servis Sağlayıcı |
| **BPF** | Bant Geçiren Filtre |
| **CA** | Sertifika Otoritesi |
| **CNN** | Evrişimli Sinir Ağları |
| **CPR** | Kompakt Konum Raporu |
| **DL** | Derin Öğrenme |
| **DNN** | Derin Sinir Ağı |
| **DSN** | Ondalık ölçekleme normalizasyonu |
| **DSSS** | Doğrudan dizili yayılı spektrum |
| **DVB-T** | Dijital Video Yayıncılığı-Karasal |
| **EEG** | Elektroensefalografi |
| **ES** | Genişletilmiş Mesaj |
| **ESA** | Avrupa Uzay Ajansı |
| **FAA** | Federal Havacılık İdaresi |
| **FHSS** | frekans atlamalı yayılı spektrum |

| Kısaltmalar | Açıklamalar |
|---|---|
| **FPE** | Biçim Korumalı Şifreleme |
| **GNSS** | Küresel Navigasyon Uydu Sistemleri |
| **HHT** | Hilbert-Huang Dönüşümü |
| **HIBE** | Hibrit Kimlik Tabanlı Şifreleme |
| **HPF** | Yüksek Geçiren Filtre |
| **I** | Faz (In-phase) |
| **IBE** | Kimlik Tabanlı Şifreleme |
| **ICAO** | Uluslararası Sivil Havacılık Örgütü |
| **KNN** | K-En Yakın Komşu |
| **LPF** | Alçak Geçiren Filtre |
| **MAF** | Hareketli Ortalama Filtre |
| **ML** | Makine öğrenmesi |
| **MMADN** | Medyan ve medyan mutlak sapma normalizasyonu |
| **NAC** | Navigasyon Doğruluk Kategorisi |
| **NextGen** | Yeni Nesil Hava Taşımacılığı Sistemi |
| **NIC** | Navigasyon Bütünlük Kategorisi |
| **OFDM** | Ortogonal Frekans Bölmeli Çoklama |
| **PKI** | Açık Anahtar Altyapısı |
| **PPM** | Darbe Pozisyon Modülasyonu |
| **PSD** | Güç Spektral Yoğunluğu |
| **Q** | Kareleme (Quadrature) |
| **RDCN** | Tekrarlanan Derin Karmaşık Değerli Ağ |
| **RF** | Radyo Frekans |
| **RFF** | Radyo Frekans Parmak izi |
| **SDR** | Yazılım Tabanlı Radyo |
| **SIBE** | Aşamalı Kimlik Tabanlı Şifreleme |
| **SIL** | Kaynak Bütünlük Seviyesi |
| **SNR** | Sinyal Gürültü Oranı |
| **SVM** | Destek vektör makinaları |
| **TBN** | Tahn Temelli Normalizasyon |
| **TCAS RA** | Trafik Çarpışma Önleme Sistemi Çözüm Önerisi |
| **TFED** | Zaman-Frekans Enerji Dağılımı |

| Kısaltmalar | Açıklamalar |
|---|---|
| **TIS-B** | Trafik Bilgi Hizmeti-Yayın |
| **UAT** | Evrensel Erişim Alıcı-Vericisi |
| **USRP** | Evrensel Yazılım Radyo Çevre |
| **VDL2** | VHF Veri Bağlantısı Modu 2 |
| **VFR** | Görerek Uçuş Kuralları |
| **VHF** | Çok Yüksek Frekans |
| **VMC** | Görsel Meteorolojik Koşullar |

# 1. GİRİŞ

Hava trafiğinin izlenmesi, havacılık endüstrisinin en temel unsurlarından birisidir. Geçmişten günümüze kadarki süreçte radar teknolojisinin bu endüstrideki önemi büyüktür. Radar sistemleri, uçakların konumlarını belirlemek, hava trafiğini güvenli bir şekilde yönlendirmek ve çeşitli havaalanları arasında koordinasyonu sağlamak amacıyla geçmişten günümüze kullanılmaktadır. Radarlar, elektromanyetik dalgaları kullanarak cisimleri tespit edebilme prensibiyle çalışırlar. Bu prensibe göre, kaynağın yaydığı elektromanyetik enerjinin bir kısmı uçaklardan yansıyarak geri gelir. Geri gelen bu yansımaların çeşitli analizleri ve hesaplamalarının sonucunda uçağın konumu hesaplanabilir. Radar teknolojisi aslen 2. Dünya Savaşı sırasında askeri amaçlar için geliştirilmiştir. Ancak, sivil havacılık alanında da hızla benimsenmiş ve geliştirilmiştir. Burada bahsedilen teknoloji, havacılıkta birincil izleme radarları olarak adlandırılan radarlardır.

Teknolojinin gelişimiyle birlikte uçakları sadece nesne olarak algılamanın yanı sıra kimlik tespitinin yapılabilmesi için bu radarları daha sonra sorgu-cevap prensibiyle çalışan ikincil izleme radarları takip etmiştir. Birincil izleme radarları tarafından tespit edilen nesnelerin kimliklerini belirlemek ve daha fazla ayrıntı sağlamak için kullanılır. Bu sayede hava trafiği kontrol sistemleri, uçakların güvenli bir şekilde belirlenen rotalarda seyahat etmelerini sağlamak için daha etkili bir şekilde çalışabilmiştir.

Otomatik Bağımlı Gözetim-Yayın (Automatic Dependent Surveillance-Broadcast, ADS-B) uçakların konum, hız, yükseklik ve diğer kritik bilgilerini otomatik olarak yayınlayan bir teknolojidir. ADS-B mesajları herhangi bir şifreleme ya da doğrulama içermeden yayınlanır. Bu durum, ADS-B yayınlarını siber saldırılara karşı daha savunmasız hale getirir. Şifrelenme veya doğrulama içermeyen ADS-B yayınları manipülasyona daha açıktır. ADS-B yayınları kopyalanıp taklit edilebilir, değiştirilebilir ya da farklı amaçlarla kullanılabilir. Sonuç olarak, sivil havacılık güvenliğini tehdit etmenin ötesinde uluslararası ilişkilerde potansiyel krizlere yol açabilir. Casus hava araçları tarafından sivil yayınlar kullanılarak aldatma faaliyetleri yürütülebilir.

Bu çalışmada ADS-B sinyallerine yönelik gerçekleştirilebilecek saldırıların tespiti amaçlanmıştır. Bunun için gerçek zamanlı ADS-B sinyalleri toplanmış, ADS-B yayın kaynaklarını ikili sınıflandırma (binary classification) yöntemi ile sınıflandırılıp

gelebilecek sahte ADS-B yayınlarının yüksek doğrulukla tespit edilebileceği görülmüştür. Destek vektör makinaları (Support Vector Machines – SVM) ile gerçekleştirilen ikili sınıflandırma yöntemiyle sınıflandırma yapılırken yazılım tabanlı radyo (Software Defined Radio, SDR) ile kaydedilmiş gerçek ADS-B sinyalleri kullanılmış kullanılmıştır. Sinyallerin, SVM ile sınıflandırılması için bazı filtrelemelere tabi tutulmuş ve benzersiz sinyal özellikleri ortaya çıkarılmıştır.

Bu çalışmanın bir diğer önemli amacı da ADS-B sistemlerinin güvenliğini artırarak havacılık endüstrisindeki güvenlik protokollerine katkıda bulunmaktır. Günümüzde, ADS-B teknolojisinin savunmasızlıklarını azaltmak ve bu sistemler üzerinden gerçekleştirilebilecek potansiyel saldırıları engellemek, havacılık güvenliği açısından kritik bir öncelik haline gelmiştir. Bu doğrultuda, ADS-B sistemlerinin daha güvenli hale getirilmesine yönelik denenmemiş bir yöntem ile çözüm sunmayı hedeflemektedir. Çalışma kapsamında elde edilen bulgular, ADS-B teknolojisinin gelecekteki gelişimine ve iyileştirilmesine yönelik değerli yönlendirmeler sağlayabilecektir. Sonuç olarak, bu araştırma, havacılık endüstrisindeki güvenlik standartlarını yükseltme ve ADS-B sistemlerinin güvenilirliğini artırma potansiyeline sahiptir.

# 2. ADS-B TEKNOLOJİSİ VE GÜVENLİ HABERLEŞME

İkinci dünya savaşından önce havacılıkta trafik henüz başlangıç aşamasındaydı. Kapsamlı hava trafik kontrol sistemlerine ihtiyaç fazla değildi çünkü çoğu uçak gündüzleri görerek uçuş kuralları (Visual Flight Rules, VFR) altında ve yalnızca görerek uçuşu mümkün kılan görsel meteorolojik koşullarda (Visual Meteorologic Conditions, VMC) yani güzel havalarda uçuyordu. Havacılığın giderek büyümesiyle birlikte hava trafik kontrolünün ilk biçimleri ışık sinyallerinin kullanılmasıyla oldu. Bunun dezavantajı pilotların yanıt verme imkanının olmamasıydı. İkinci Dünya Savaşıyla birlikte oldukça gelişen radar ve transponder[1] sistemleri havacılıkta kullanılmaya başlanmış ve artan hava trafiğinin düzenlenmesinde etkin rol oynamıştır. Ancak, giderek artan sıkışıklık nedeniyle Federal Havacılık İdaresi'nin (Federal Aviation Administration, FAA) Yeni Nesil Hava Taşımacılığı Sistemi programı (Next Generation Air Transportation System, NextGen) ve Avrupa Uzay Ajansı'nın (European Space Agency, ESA) Tek Avrupa Gökyüzü (Single European Sky) gibi programları hava sahası modernizasyonu için çalışmaktadır. Bu programlar, iletişim açısından ses tabanlı radyo iletişiminden dijital veri bağlantılarına geçişin gerçekleşmesi amaçlarındadırlar. Gözetleme sistemleri otomatik bağımlı gözetlemeye geçişte, gözetleme verilerini herhangi bir radara bağımlı olmadan GPS gibi uydu verilerini sağlayacağı anlamına gelmektedir (Nolan, 2011:36,41).

Bu yapılacak değişiklikler ve iyileştirmeler, siber güvenlik açısından bazı sorunları da beraberinde getirmektedir. Bu bölümde, havacılıkta kullanılan gözetim sistemlerinden olan ADS-B teknolojisinin sistem mimarisi, yayın sıklığı, mesaj içerikleri, güvenlik problemlerinden ve bunlara yönelik çözüm önerilerinden bahsedilecektir.

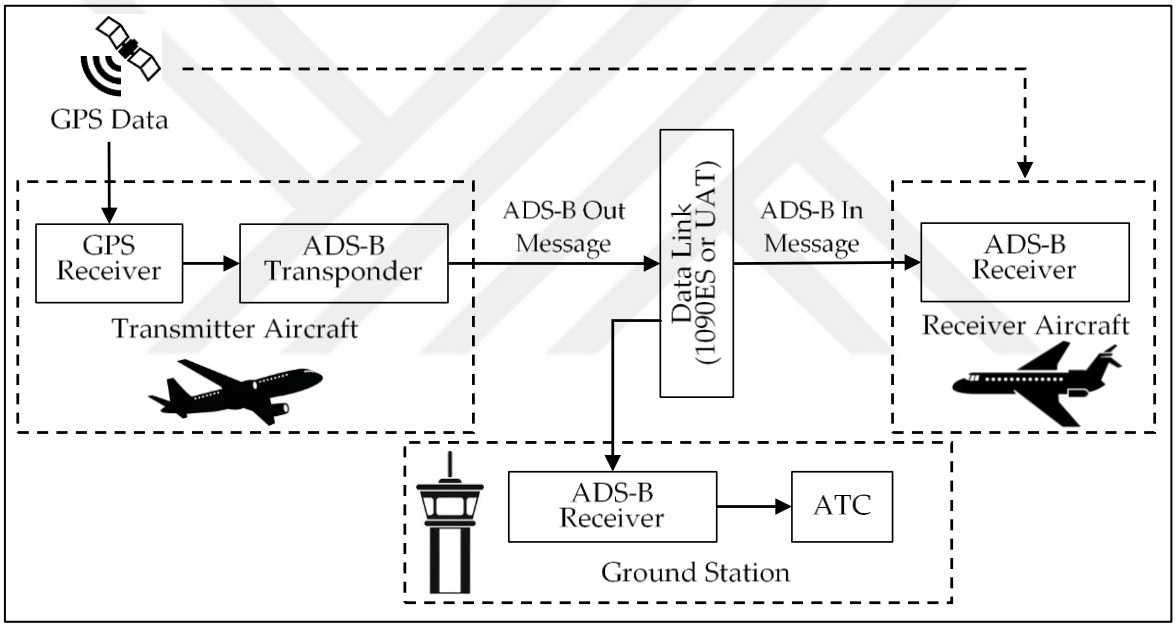
## 2.1. ADS-B Teknolojisi

Havacılıkta dalında gözetim sistemi, hava araçlarının hareketlerini ve konumlarını izleme sürecini ifade eder. Bu kapsamlı sistem, hava trafik kontrol sistemleri, radarlar, uydu tabanlı izleme sistemleri ve diğer teknolojileri içerir. Havacılık gözetimi, genellikle güvenli uçuşlar sağlamak, verimli bir hava trafik akışı sağlamak ve hava araçlarının birbiriyle ve çevreleriyle olabilecek çatışmalarını tespit edip engellemek amacıyla hayati bir role sahiptir. ADS-B teknolojisi de gelişmiş bir gözetim uygulamasıdır.

[1]Transponder: hava araçlarında bulunan, radyo frekansı ile sorgulandığında bir yanıt üreten ve yayınlayan elektronik cihaz

### 2.1.1. ADS-B sistemi ve genel tasarımı

Teknolojinin gelişmesiyle birlikte hava yolu yolculuğu da önemli derecede artış göstermiştir. Bu artışın kontrolünün sağlanabilmesi için de önemli teknolojik gelişmeler ortaya çıkmıştır. Günümüzde hava trafiğinin kontrol edilmesine en büyük katkıyı sunan teknolojilerden birisi ADS-B teknolojisidir. ADS-B hava araçlarının konum ve diğer bilgilerini belirleyip düzenli aralıklarla yayınlamasını sağlayan bir teknolojidir. Bu sayede hava araçları, birbirleri ve hava trafik kontrol sistemleriyle otomatik olarak iletişim kurabilmekteler. ADS-B teknolojisi, hava trafiğindeki çatışmaların önlenmesine yardımcı olarak hava trafik yönetiminde daha etkili bir izleme ve iletişim sistemini imkânı sunar.




Şekil 2.1. ADS-B sisteminin ana bileşenleri ve sistem akışı

ADS-B'nin açılımında bulunan *otomatik*; konum, hız vb. bilgileri, uçuş ekibi veya operatör girişi olmadan periyodik olarak otomatik olarak gönderilmesinden gelir. Gönderilecek parametreler önceden seçilir ve statiktir. *Bağımlı*, yayını yapan hava aracının konumunu, süratini ve kullanılabilirliğini belirleyen ekipmanların (kendi donanımlarının) düzgün çalışmasına bağlıdır. Yani hava taşıtları ADS-B için kendi donanımlarına güvenirler. *Gözetim*; pozisyon, sürat, yükseklik ve hava aracına ait diğer bilgiler iletilen gözetim verileri anlamındadır. *Yayın*; mesaj bilgileri, ADS-B alıcısı olan herhangi bir hava aracı veya yer istasyonuna periyodik olarak yayınlanması anlamındadır (Soyertem, 2022:52,53).

Amerikan Federal Havacılık İdaresi (Federal Aviation Administration, FAA) Haziran 2010'da "Title 14 Code of Federal Regulations (CFR)" kapsamında bir düzenleme yayınladı. Bu düzenlemeye göre belirli hava sahalarında elektrik sistemi olan tüm uçaklar için 1 Ocak 2020'ye kadar ADS-B Out donanımını zorunlu hale getirdi. Avrupa Komisyonu, Tek Avrupa Gökyüzü'nü (Single European Sky) zorunlu kılan 1207/2011 sayılı Yönetmeliği yayınladı. Bu yönetmeliğe göre 8 Ocak 2015'ten sonra inşa edilen uçaklar için ADS-B Out kullanımını zorunlu hale getiriyor. Ayrıca, halihazırda kullanımda olan tüm uçaklar için son tarih olarak 7 Aralık 2017'yi belirlemiştir. Ancak, bu son dönüşüm tarihini önce 2020'ye, daha sonra 2023 ve 2025 yıllarına erteleyip eski uçakların geçişleri için ekstra muafiyetler eklemiştir (Sun ve diğerleri, 2021).

ADS-B iki yönlü iletişim sağlar. Bu da sadece uçakların veri yayınlamasıyla sınırlı olmadığı anlamına gelir. Ayrıca, diğer hava araçları ve hava trafik kontrol sistemleriyle de iletişim kurma yeteneğine sahiptir. ADS-B yayını yapan hava aracı aynı zamanda kapsama alanında bulunan hava araçları tarafından izlenebilir.

ADS-B sistem mimarisi hava aracının aviyonik sistemlerinden ve Hava Trafik Servis Sağlayıcı (Air Traffic Service Provider, ATSP) dan oluşur. ADS-B aviyoniklerinin 2 farklı çalışma modu bulunur. Bunlar ADS-B IN ve ADS-B OUT dur. ADS-B aviyonikleri aynı anda her iki bilgiye de erişebilmektedir. ADS-B Out, ADS-B bilgilerinin yayınlanması-gönderilmesi işlemine denir. ADS-B-In, ADS-B bilgilerinin alınması işlemine denir. Hava aracında bulunan "konum kaynağı" genellikle Küresel Navigasyon Uydu Sistemlerini (Global Navigation Satellite System – GNSS) kullanarak konum bilgilerini ADS-B ile donatılmış uçaklara ve yer istasyonlarına iletir. ABD'de 1090 MHz ve 978 MHz olmak üzere 2 farklı frekansta yayın sağlar. Mode A, C ve S transponderleri, 1090 MHz frekansında çalışırlar ve bu frekansta yayınlanan sinyaller '1090 Extended Squitter' (Genişletilmiş Mesaj, ES) olarak bilinir. Bu transponderler çoğunlukla yüksek irtifada uçan uçaklar tarafından kullanılır. Diğer taraftan, 978 MHz frekansında çalışan 'Universal Access Transceiver' (UAT) sistemleri, genellikle FL180 (Flight Level 180, yaklaşık 18,000 feet yükseklik) seviyesinin altında uçan hava araçları için tasarlanmıştır (Surveillance and Broadcast Services Description Document, 2018: 5).

### 2.1.2. ADS-B yayın sıklığı

ADS-B yayınları belirli periyotlara göre kesintisiz devam etmektedir. Bu mesajlar farklı içeriklere göre farklı yayın sıklığına sahiptir. Bu yayın sıklığı uçağın yerde mi havada mı olduğuna, yerde ise hareketli mi hareketsiz mi olduğuna göre değişiklik göstermektedir.

Çizelge 2.1. ADS-B mesajlarının güncellenme sıklığı (Sun, 2021:38)

<table>
<tr><th>Mesaj</th><th>Tip Kodu</th><th>Yer (Sabit)</th><th>Yer (Hareketli)</th><th>Hava</th></tr>
<tr><td>Uçak Kimliği</td><td>1-4</td><td>0.1 Hz</td><td>0.2 Hz</td><td>0.2 Hz</td></tr>
<tr><td>Yeryüzü Konumu</td><td>5-8</td><td>0.2 Hz</td><td>2 Hz</td><td>-</td></tr>
<tr><td>Seyir Konumu</td><td>9-18, 20-22</td><td>-</td><td>-</td><td>2 Hz</td></tr>
<tr><td>Seyir Hızı</td><td>19</td><td>-</td><td>-</td><td>2 Hz</td></tr>
<tr><td rowspan="2">Uçak Durumu</td><td rowspan="2">28</td><td colspan="3">0.2 Hz (TCAS RA ve Squawk Kodu değişikliği yok)</td></tr>
<tr><td colspan="3">1.25 Hz (TCAS RA veya Squawk Kodu değişir)</td></tr>
<tr><td>Hedeflenen ve Mevcut Durum</td><td>29</td><td>-</td><td>-</td><td>0.8 Hz</td></tr>
<tr><td rowspan="2">Operasyonel Durum</td><td rowspan="2">31</td><td rowspan="2">0.2 Hz</td><td colspan="2">0.4 Hz (NIC/NAC/SIL değişikliği olmaz)</td></tr>
<tr><td colspan="2">1.25 Hz (NIC/NAC/SIL’da değişir)</td></tr>
</table>

Burada bahsedilen Hz (Hertz) frekans birimidir ve saniyede gerçekleşen yayın sıklığı demektir. Buna göre, 2 Hz yayın sıklığına ait olan yeryüzü konumu bilgisi, saniyede 2 defa yayınlandığını göstermektedir.

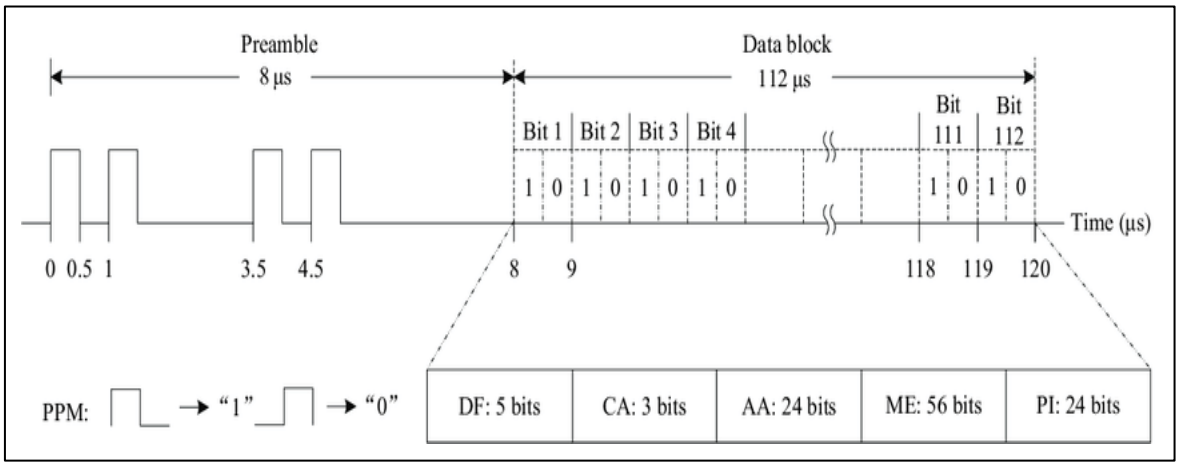
### 2.1.3. ADS-B 1090ES mesaj formatı

Mode-S sinyallerinin içeriğinde ADS-B mesajları da bulunur. Downlink Format 17 ve 18 olan mesajlar ADS-B mesajlarını belirtir. Mode-S transponderına sahip hava araçları Downlink Format (DF) 17’yi kullanırken Mode-S transponderi olmayan hava araçları Trafik Bilgi Hizmeti-Yayın (Traffic Information Service – Broadcast, TIS-B) adı verilen yayın kaynağı vasıtasıyla DF 18’i kullanarak mesaj yayınlar. Bu sayede DF18 ile gelen yayını alan alıcı, bu mesajın kaynağında sorguya cevap verebilme kabiliyeti olmadığını anlar (Bostancı, 2021:14). ADS-B mesajları 8 bit preamble ve 112 bilgi mesajı olmak üzere toplam 120 bittir. Bu mesaj Çizelge 2.2’de belirtilen 5 bölümden oluşmaktadır.

Çizelge 2.2. 1090ES Mesaj İçeriği (Sun, 2021:35)

| Bit Sayısı | Bit Aralığı | Kısaltması | Açıklaması |
|---|---|---|---|
| 5 | 1-5 | DF | Downlink Formatı |
| 3 | 6-8 | CA | Transponder Kabiliyeti |
| 24 | 9-32 | ICAO | ICAO Adresi |
| 56 | 33-88 | DATA | Mesaj (veri) |
| | 33-37 | TC | Mesaj Tip Kodu |
| 24 | 89-112 | PI | Parite |

İlk mesaj alanındaki 5 bit, 1090ES Mode-S vericisi tarafından Downlink Formatını belirtir. 1090ES yayınlarında DF 17'yi kullanır. İkinci mesaj alanı 3 bit ile transponder seviyesini gösteren Transponder Kabiliyeti'ni (Capability) gösterir. Sonraki 24 bit hava aracının Uluslararası Sivil Havacılık Örgütüne göre özgün kimlik kodunu yani ICAO (International Civil Aviation Organization) kodunu gösterir ve teorik olarak hava aracının çalışabilir ömrü boyunca değişmez. Sonraki 56 bit mesaj içeriği gösterir. Bu kısımda pozisyon hız ve diğer bilgiler içerir. Son 24 bit ise parite olarak ayrılmıştır. ADS-B mesajları Darbe Pozisyon Modülasyonu (Pulse Position Modulation, PPM) modülasyon işlemine tabi tutulmaktadır.




Şekil 2.2. 1090ES data link formatı (Ren, Wang, Song, Zhang ve Ban, 2016)

### 2.1.4. Kapasite

Kapasite, ADS-B mesajının ikinci kısmındaki 3 bitlik alanı temsil eder. Bu alan transponder seviyesini gösterir. Transponder seviyesi 0 ile 7 arasında bir değer alabilir. Bu değerlerin anlamları Çizelge 2.3'de sunulmuştur.

Çizelge 2.3. Kapasite değerleri karşılıkları (Sun, 2021:36)

| Kapasite | Tanım |
|---|---|
| 0 | Seviye 1 Transponderi |
| 1-3 | Rezerve ayrılmıştır |
| 4 | Seviye 2+ Transponderi, Yer |
| 5 | Seviye 2+ Transponderi, Hava |
| 6 | Seviye 2+ Transponderi Hem Hava Hem Yer |
| 7 | Hava ya da yerde Downlink talebinin 0, uçuş durumunun 2, 3, 4, 5 olduğunu belirtir. |

### 2.1.5. ICAO Kodu

Uluslararası Sivil Havacılık Örgütü (International Civil Aviation Organization, ICAO), Birleşmiş Milletlere bağlı bir kuruluş olup uluslararası sivil havacılık standartlarıyla beraber yönetmeliklerini belirlemek, düzenlemek ve koordine etmekten sorumludur. ICAO, sivil havacılıkla ilgili konularda tüm dünya genelinde bir standart oluşturarak, hava taşımacılığı güvenliği, etkinliği ve sürdürülebilirliği teşvik etmeyi amaçlar.

ADS-B mesajlarında hava araçlarına ait ICAO kodu 24 bittir ve 16777214 farklı ICAO kodundan birisidir. Bu kodun atanması için bazı prensipler vardır. Bunlar:

- Hiçbir ICAO adresi, birden fazla uçağa atanmamalıdır;
- Bir hava aracına taşıdığı ekipman bileşiminden bağımsız olarak sadece 1 adres atanmalıdır;
- Adres istisnai durumlar dışında değiştirilmemeli, uçuş sırasında değiştirilmemelidir;
- Bir adres değiştirildiğinde önceki atanmış adres bırakılmalı ve yeni kaydeden otorite tarafından yeni bir adres atanmalıdır;
- Adres sadece uçakları tanımlama amacıyla teknik bir role sahip olmalı ve herhangi bir özel bilgi taşımamalıdır;
- 24 adet 0 ya da 1’ den oluşan adresler uçaklara atanmamalıdır.

şeklinde 6 adet temel kural tanımlanmıştır (ICAO Annex 10 Volume III Chapter 9. Aircraft Addressing System, 2007:2).

### 2.1.6. ADS-B mesaj tip kodları

112 bitlik ADS-B verisinde Downlink Formatı, Transponder Kabiliyeti ve ICAO adresinden sonra 56 bitlik mesaj kısmı gelir. Çizelge 2.3'de görüldüğü gibi mesaj içeriğinde uçak kimliği, yeryüzü konumu, seyir konumları, seyir hızı, uçak durumu, hedef durumu ve mevcut durum bilgisi ve uçağın operasyonel durumu yer almaktadır. Bu tip kodunda yer alan bilgiye göre ADS-B mesajının içerdiği verinin bilgisi anlaşılabilir.

Çizelge 2.4. ADS-B Mesajlarının Tip Kodları ve İçerikleri (Sun, 2021:37)

| Tip Kodu | Mesaj İçeriği |
|---|---|
| 1-4 | Uçuş Kimliği |
| 5-8 | Yeryüzü Konumu |
| 9-18 | Seyir Konumu (Barometrik İrtifa Bilgisiyle) |
| 19 | Seyir Hızı |
| 20-22 | Seyir Konumu (GNSS İrtifa Bilgisiyle) |
| 23-27 | Rezerve |
| 28 | Uçak Durumu |
| 29 | Hedef Durum ve Mevcut Durum Bilgileri |
| 30 | Rezerve |
| 31 | Uçağın Operasyonel Durumu |

### 2.1.7. ADS-B uçuş kimliği paketi

Uçağın çağrı adı ile kategorisini bildirmek için yayınlanan mesajlardır. Uçağın çağrı adı ICAO kodu gibi benzersiz bir kimlik değildir. Bu mesajda ADS-B Tip Kodu 1 ile 4 arasında bir değer alır. 56 Bitlik mesaj paketi 10 parçadan oluşur. Bu 10 parça;

Çizelge 2.5. ADS-B uçak kimliği mesaj paketinin içerik dağılımı

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| TC, 5 | CA, 3 | C1, 6 | C2, 6 | C3, 6 | C4, 6 | C5, 6 | C6, 6 | C7, 6 | C8, 6 |

TC: Tip Kodu
CA: Kapasite
C*: Karakter

olarak temsil edilmektedir. Buradaki 6 sayısı karakterlerin her birini kodlamak için kullanılan bit sayısını temsil eder. Mesajda uçağın çağrı adı bulunur ancak bu çağrı adı,

farklı zamanlarda aynı rotada uçan farklı uçaklar arasında benzersiz bir tanımlayıcı değildir. Farklı uçaklar aynı çağrı adını kullanabilir. Bu diyagramda gösterilen son 8 bit alanı çağrı adını temsil eder. Bu 8 bitlik alanlar 6'şar bit içerir. Karakterlerin çözülebilmesi için Çizelge 2.6'daki çevrim tablosuna ihtiyaç duyulur.

Çizelge 2.6. Karakter çözümlemesi için gerekli çevrim tablosu

| #ABCDEFGHIJKLMNOPQRSTUVWXYZ##### ###############0123456789######<br>A - Z : 1 - 26<br>0 - 9 : 48 - 57<br>␣(boşluk) : 32 |
|---|

İlk olarak, # kullanılmayan olarak belirtilir. Bu kodlama ASCII (American Standard Code for Information Interchange) ile var olanın 6 karakter altını belirterek kodlanır. Kapasite bit alanı Tip Koduyla birlikte aşağıdaki gibi yorumlanabilir.

Çizelge 2.7. Tip Kodu ve Kapasitenin birlikte karşılıkları (Sun, 2021:42)

| Tip Kodu | Kapasite | Kategori |
|---|---|---|
| 1 | X | Rezerve |
| X | 0 | Kategori Bilgisi Yok |
| 2 | 1 | Acil Durum Yer Aracı |
| 2 | 3 | Yer Hizmet Aracı |
| 2 | 4-7 | Yüzey Engelleri |
| 3 | 1 | Yelkenliler ve Planörler |
| 3 | 2 | Havadan Hafif |
| 3 | 3 | Gök Dalışçısı - Paraşüt |
| 3 | 4 | Ultralight, Planör, Yamaç Paraşütü |
| 3 | 5 | Rezerve |
| 3 | 6 | İnsansız Hava Aracı |
| 3 | 7 | Uzay ya da Trans Atmosferik Araç |
| 4 | 1 | Hafif (7000 kg'dan az) |
| 4 | 2 | Orta 1 (7000 kg ile 34000 kg arası) |
| 4 | 3 | Orta 2 (34000 kg ile 136000 kg arası) |
| 4 | 4 | Yüksek Vortex Uçağı |
| 4 | 5 | Ağır (136000 kg'den büyük) |
| 4 | 6 | Yüksek Performans (>5 g ivmelenme) ve Yüksek Hız (>400 kt) |
| 4 | 7 | Döner Kanat (Rotorlu) Hava Aracı |

### 2.1.8. Seyir konumu

Uçağın havadaki konumu ve irtifasına ilişkin bilgileri yayınlayan mesajlardır. Mesaj yapısı sekiz parçadan oluşur, bkz. Çizelge 2.8.

Çizelge 2.8. Havadaki konum mesaj paketinin içerik dağılımı

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| TC, 5 | SS, 2 | SAF, 1 | ALT, 12 | T, 1 | F, 1 | LAT-CPR, 17 | LON-CPR, 17 |

Bu sekiz parçadan oluşan havadaki konum bilgisini içeren ADS-B mesajına ilişkin detaylar Çizelge 2.9'da gösterildiği gibidir.

Çizelge 2.9. Havadaki konum mesaj paketinin yapısı (Sun, 2021:45)

| Parça | | MSG | ME | BITS |
|---|---|---|---|---|
| Tip Kodu (Type Code)<br>9-18: barometrik irtifa<br>20-22: GNSS irtifa | TC | 33-37 | 1-5 | 5 |
| Gözetim Durumu (Surveillance Status)<br>0: Durum bilgisi yok<br>1: Kalıcı uyarı<br>2: Geçici uyarı<br>3: SPI durumu | SS | 38-39 | 6-7 | 2 |
| Tek Anten Bayrağı (Single Antenna Flag) | SAF | 40 | 8 | 1 |
| Kodlanmış İrtifa (Encoded Altitude) | ALT | 41-52 | 9-20 | 12 |
| Süre (Time) | T | 53 | 21 | 1 |
| CPR Formatı<br>0: even frame<br>1: odd frame | F | 54 | 22 | 1 |
| Kodlanmış CPR Enlem (Encoded Latitude) | LAT-CPR | 55-71 | 23-39 | 17 |
| Kodlanmış CPR Boylam (Encoded Longitude) | LON-CPR | 72-88 | 40-56 | 17 |

Mesajdaki tip kodu 9-18 aralığında ise uçağın barometrik irtifa bilgisi, 20-22 aralığında ise GNSS irtifa bilgisi yayınlanmaktadır. Vurgulanması gereken diğer bir nokta ise kodlanmış enlem ve boylam bilgilerinin gerçek enlem ve boylam bilgisini değil, Kompakt Konum Raporu (Compact Position Reporting, CPR) formatında kodlanmış enlem ve boylam bilgisini yayınlamasıdır. CPR formatının tercih edilme sebebi daha az bit kullanarak daha net çözümler sağlamasıdır.

### 2.1.9. Yeryüzündeki konum

Uçak yeryüzünde iken, konum bilgisine ilişkin mesaj tipi havada iken yayınlanan mesaj tipinden farklılık gösterir. Havadaki konum mesajından farklı olarak, yeryüzündeki konum mesajı irtifa bilgisi yerine ayrıca uçağın hız ve yeryüzünde izlediği yol bilgisini içerir.

Mesaj yapısı sekiz parçadan oluşur, bkz. Çizelge 2.10.

Çizelge 2.10. Yerdeki konum mesaj paketinin içerik dağılımı

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| TC, 5 | MOV, 7 | S, 1 | TRK, 7 | T, 1 | F, 1 | LAT-CPR, 17 | LON-CPR, 17 |

Bu sekiz parçadan oluşan yeryüzündeki konum bilgisini içeren ADS-B mesajına ilişkin detaylar Çizelge 2.11'de gösterildiği gibidir.

Çizelge 2.11. Yerdeki konum mesaj paketinin yapısı (Sun, 2021:61)

| Parça | | MSG | ME | BITS |
|---|---|---|---|---|
| Tip Kodu (Type Code) | TC | 33-37 | 1-5 | 5 |
| Hareket (Movement) | MOV | 38-44 | 6-12 | 7 |
| Ground Track Durumu (Status for Ground Track)<br>0: Geçersiz<br>1: Geçerli | S | 45 | 13 | 1 |
| Ground Track | TRK | 46-52 | 14-20 | 7 |
| Süre (Time) | T | 53 | 21 | 1 |
| CPR Format<br>0: even frame<br>1: odd frame | F | 54 | 22 | 1 |
| Kodlanmış Enlem (Encoded Latitude) | LAT-CPR | 55-71 | 23-39 | 17 |
| Kodlanmış Boylam (Encoded Longitude) | LON-CPR | 72-88 | 40-56 | 17 |

Buradaki hareket, uçağın yerdeki hızını ifade ederken, yeryüzünde izlediği yol ise yerdeki yön bilgisi ile ilgilidir.

### 2.1.10. Seyir hızı

Uçağın havadaki hızı bilgisini yayınlayan mesaj paketidir. Havadaki hız bilgisi için tip kodu her zaman 19 (TC=19)'dur. Havadaki hız mesaj paketinin genel yapısı Çizelge 2.12'deki gibidir.

Çizelge 2.12. Havadaki hız mesaj paketinin yapısı (Sun, 2021:69)

| Parça | | MSG | ME | BITS |
|---|---|---|---|---|
| Tip Kodu (Type Code)<br>TC=19 [Binary: 10011] | TC | 33-37 | 1-5 | 5 |
| Alt-tip (Sub-type) | ST | 38-40 | 6-8 | 3 |
| Niyet Değişim Bayrağı (Intent Change Flag) | IC | 41 | 9 | 1 |
| IFR Kapasitesi Bayrağı (IFR Capability Flag) | IFR | 42 | 10 | 1 |
| Hız için Navigasyon Belirsizlik Kategorisi (Navigation Uncertainty Category for Velocity)<br>ADS-B versiyon 0<br>ADS-B versiyon 1-2 | <br>NUCr<br>NUCv | 43-45 | 11-13 | 3 |
| Alt-tipe özel parçalar (Sub-type Specific Fields) | F | 46-67 | 14-35 | 22 |
| Düşey Hız için Kaynak (Source Bit for Vertical Rate) | VrSrc | 68 | 36 | 1 |
| Düşey Hız için İşaret (Sign Bit for Vertical Rate) | Svr | 69 | 37 | 1 |
| Düşey Hız (Vertical Rate) | VR | 70-78 | 38-46 | 9 |
| Rezerve (Reserved) | | 79-80 | 47-48 | 2 |
| GNNS ve Barometrik İrtifa Farkı için İşaret (Sign Bit for GNSS and Baro altitudes difference) | SDiff | 81 | 49 | 1 |
| GNSS ve Barometrik İrtifa Farkı (Difference between GNSS and Baro altitudes) | dAlt | 82-88 | 50-56 | 7 |

Çizelge 2.14'de görüldüğü gibi, 6-8 aralığındaki mesaj bitleri mesajın alt-tiplerini tanımlar. Dört farklı alt-tip mevcuttur. Bunların her biri benzer bir mesaj yapısına sahip olmakla birlikte, 14-35 aralığındaki mesaj bitleri ile tanımlanan farklılıklar gösterebilir.

Uçağın yerdeki hızı alt-tip 1 ve 2 ile gösterilir. Uçağın konumu GNSS sistemi tarafından belirlenemediğinde ise alt-tip 3 ve 4 ile uçağın havadaki hızı bilgisi yayınlanır. Gerçek hayatta, alt-tip 3 mesajları oldukça nadir görülür.

Bu mesajlar yatay ve düşey hız bilgisinin yanında, iki önemli bilgi daha içerirler. Bunlar hız için navigasyon belirsizlik kategorisi ve GNSS yüksekliği ile barometrik irtifa arasındaki fark bilgileridir.

Konum mesajlarından farklı olarak, hız mesajları karmaşık kodlama şemaları içermediğinden çözümlenmesi daha kolaydır.

### 2.1.11. Uçağın operasyonel durumu

Uçak ile ilgili çeşitli bilgileri yayınlayan mesajlardır. Tip kodu 31 (TC=31)'dir. Farklı ADS-B versiyonları için mesaj yapıları önemli farklılıklar göstermektedir. Bu mesaj paketi bütün ADS-B versiyonları için tanımlanmıştır, ancak pratikte versiyon 0 için oldukça az uygulanır. Versiyon 1 ve sonrası için, operasyonel durum mesajı ADS-B versiyonu, netlik ve bütünlük göstergeleri gibi bilgiler içerir.

### 2.1.12. ADS-B hata kontrolü

Dijital haberleşme sistemlerinde hata kontrolü oldukça önemlidir. Hata kontrol kodlama şemaları, alıcının gelen bilgiyi doğrulamasını ve gerektiğinde var olan hataları düzeltmesini sağlamalıdır. İletişim kanalının ve mesaj tiplerinin özelliklerine göre, farklı hata kontrol kodlama şemaları uygulanabilir.

Hataların belirlenmesi için, üç farklı hata kontrol kodlama şeması yaygın olarak kullanılmaktadır: *i)* parity, *ii)* checksum ve *iii)* cyclic reducdancy check (CRC). Bu üç şema benzerlik gösterse de önemli ayırt edici özellikleri mevcuttur. En kolay uygulanabilir olan şema parity iken, hataların belirlenmesinde en başarılı olan şema CRC'dir. CRC aynı zamanda hataların düzeltilmesine de imkân sağlar.

### 2.1.13. Mesaj çözümleme örneği

ADS-B alıcısının aşağıdaki ham veriyi yakaladığını düşünelim.

Ham veri: 8D4840D6201C168914564C576098 (HEX)

Bu ham verideki ilk iki onaltılık bölüm DF ve CA'yı ifadeeder. Ardından gelen altı onaltılık uzunluğundaki bölüm ICAO kodunu belirtir. İzleyen on dört onaltılık uzunluğundaki bölüm mesajın içeriğini barındırırken, son altı onaltılık bölüm parite için ayrılmıştır.

Çizelge 2.13. Ham verinin (HEX) Çözümlenmesi

| HEX | 8D | 4840D6 | 201C168914564C | 576098 |
|---|---|---|---|---|
| BIN | 10001 101 | 010010000100 000011010110 | 00100000000111000000101101000 10010001010001010110010011 00 | 010101110110 000010011000 |
| DEC | 17 5 | | | |
| DESC | DF CA | ICAO Kodu | Mesaj Bölümü | Parite |

Burada görüldüğü üzere ilk 5 bit ile DF, sonraki 3 bit ile CA bilgisi iletilmiştir. Burada DF: 17 bize ADS-B mesajı olduğu bilgisini iletir. CA:5 ise seviye 2+ havadan gelen bir mesaj olduğunu iletir. Mesaj bölümünün çözümlenmesi bölümlerine ayrılırsa;

Çizelge 2.14. Mesaj kısmının çözümlenmesi

| TC, 5 | CA, 3 | C1, 6 | C2, 6 | C3, 6 | C4, 6 | C5, 6 | C6, 6 | C7, 7 | C8, 8 |
|---|---|---|---|---|---|---|---|---|---|
| 00100 | 001 | 000111 | 000001 | 011010 | 001001 | 000101 | 000101 | 011001 | 001100 |
| 4 | 1 | 7 | 1 | 26 | 9 | 5 | 5 | 25 | 12 |
| 4 | 1 | G | A | Z | I | E | E | Y | L |

Burada Tip kodu 4 olarak verilmiş. Bu da mesaj içeriğinin uçak kimliğini içereceğini göstermektedir. CA verisi, TC ile birlikte 41 olarak bize “Hafif (7000kg’dan az)” tipinde bir uçak olduğu bilgisini iletmektedir. Uçak kimliği tarafımca Gazi Üniversitesi Elektrik Elektronik Mühendisliği Yüksek Lisansına atıfta bulunarak “GAZIEEYL” olarak oluşturulmuştur.

## 2.2. ADS-B Güvenlik Sorunları

ADS-B teknolojisi hava trafik kontrol (Air Traffic Control, ATC) sistemlerinin verimliliğini artırmak, uçuş güvenliğini iyileştirmek ve hava taşımacılığını daha sürdürülebilir hale getirmek için hayati bir rol oynamaktadır. ADS-B sistemi, geleneksel radar sistemlerine göre daha keskin ve güncel konum bilgileri sağlayarak trafik kontrolörüne daha yüksek çözünürlük sağlar. Bu da trafik yönetim kolaylığının yanında, daha yüksek güvenlik de sağlar.

Bağımsız Hava Trafik Yönetimi'nden (Air Traffic Management-ATM) bağımlı bir forma geçiş ve ADS-B'nin tanıtılıp kullanılmasıyla birlikte, bazı güvenlik zafiyetleri de ortaya

çıkmaktadır. ADS-B protokolü, herhangi bir şifreleme ve kimlik doğrulama yöntemi sunmaz ve çeşitli siber saldırılara maruz kalabilir (McCallie, Butts ve Mills, 2011), (Leonardi, Piracci ve Galati, 2014). ADS-B, güvenliği birincil öncelik alarak tasarlanmamıştır. Bu nedenle kolayca elde edilebilen donanım ve yazılım kullanılarak saldırıya uğrayabilir (Strohmeier, Lenders ve Martinovic, 2013). SDR cihazları herkesin düşük maliyetle RF iletimlerini alıp göndermesini kolaylaştırır. Bu, şifrelenmemiş ADS-B protokolünü saldırılara daha açık hale getirir (Zhijun, Tong ve Anxin, 2017). Ayrıca, araştırmalar tarafından ADS-B sistemi üzerinde bir dizi saldırının zaten başarıyla gerçekleştirildiği gösterilmiştir. Schafer, Lenders ve Martinovic (2013), SDR kullanarak ADS-B sistemine bir hayalet uçağın (sahte uçak) enjekte edilmesini başarıyla gerçekleştirmiştir.

Manesh ve Kaabouch (2017), saldırıların gerçekleştirilme olasılıkları ve etkileri göz önünde bulundurularak ADS-B zafiyetlerinin bir risk analizini temsil eden Çizelge 2.15'i oluşturmuştur. Yüksek, orta-yüksek, orta ve düşük riskler sırasıyla kırmızı, turuncu, sarı ve yeşil renklerle temsil edilmektedir.

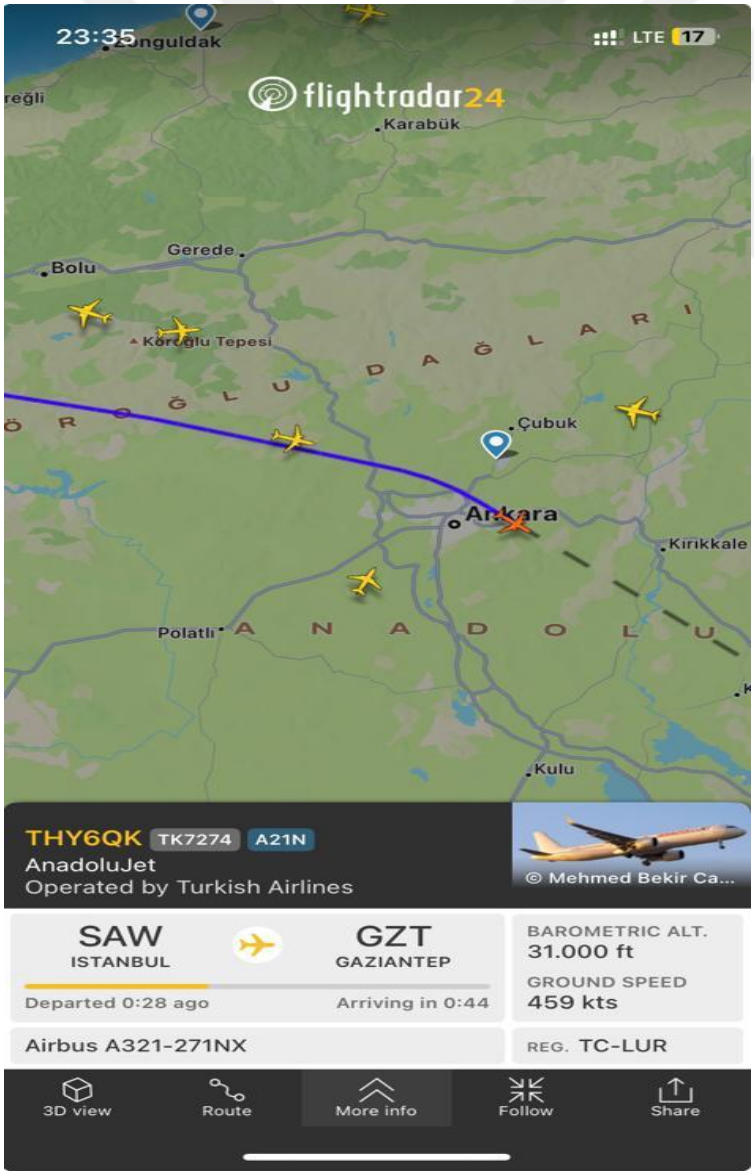
Çizelge 2.15. ADS-B saldırılarındaki risk analizi

| | | Saldırı Etkisi | | |
|---|---|---|---|---|
| | | Düşük | Orta | Yüksek |
| Saldırı Olasılığı | Yüksek | Kolay Dinlenebilme | | |
| | Orta | | Karıştırma | Mesaj Yerleştirme |
| | Düşük | | Mesaj Silme | Mesaj Değiştirme |

ADS-B sisteminin saldırılara karşı savunmasızlığı ve kolaylığı, bu güvenlik sorunlarını azaltma ihtiyacını ortaya çıkarmaktadır. Mirzaei, Carvalho ve Pschorn (2019) tarafından tanımlanan bir dizi güvenlik tehdidi ve gereksinimi bulunmaktadır. Bu güvenlik tehditlerini Louwen (2022), tez çalışmasında 5 farklı temelde ADS-B güvenlik sorunu olarak açıklamıştır.

### 2.2.1. Kolay dinlenebilme (eavesdropping)

ADS-B iletilen mesajlarda şifreleme kullanmadığı için, veri alışverişi kolayca dinlenebilir. Ancak, bu zafiyetin kendisi hava trafik kontrol sistemine zarar vermez ve bu nedenle en az etkiye ve en düşük riske sahiptir. Herhangi bir ADS-B alıcısı olan herkes bu sinyalleri okuyabilir. Bu kadar kolay elde edilebilir olması daha çok saldırı planlanmasına yönelik bazı kolaylıklar da sağlayabilir. ADS-B verilerinin toplanması düşman olmayan aktörler tarafından da gerçekleştirilir. Bu verileri görselleştiren platformlar mevcuttur ve bu platformlar geçmişe yönelik uçuşlara dair detayları da ücretli/ücretsiz olarak sunmaktadır. Bu platformlardan bazıları Flighradar24, Planetfinder, FlightAware ve RadarBox'dur.




Şekil 2.3. Canlı olarak konum, hız, yükseklik vb. verilerin takip edilebildiği FlightRadar uygulaması görseli

### 2.2.2. Mesaj yerleştirme (message injection)

ADS-B mesajlarında hiçbir doğrulama, kriptolama veya yetkilendirme bulunmadığı daha önceki bölümlerde belirtilmiştir. Bu durum saldırganların sisteme sahte mesajlar oluşturup enjekte etmesine olanak sağlar. ADS-B mesajı kendi 3D konum bilgisini gönderdiği için ADS-B alıcısı alınan mesajın konumunun gerçek ADS-B vericisine ait olup olmadığını doğrulayamaz. Bir ADS-B mesajının tamamını oluşturup enjekte etmek, aslında var olmayan hayalet uçağı temsil eden bir mesaj gibi görünecektir. Mesaj Enjekte saldırısının yüksek doğrulukla tahmin edilebildiği çalışmalar olsa da standart bir ADS-B alıcısı gerçek ve sahte mesajları ayırt edemez. Bu yayın ile gönderilen konumun gerçek olup olmadığını doğrulayamaz. Slimane, Benouadah, Shamaileh, Devabhaktuni ve Kaabouch, (2022) çalışmasında bu tür saldırılara karşı sistemin savunmasızlığını enjekte edilen ADS-B mesajı ile göstermiştir.

ATC sistemine sahte ADS-B mesajları enjekte etmek, karmaşık ve potansiyel olarak oldukça tehlikeli durumlar yaratabilir. Bu durumlar arasında gereksiz seyahat, hatalı yola yönlendirmeler ve Hava Çarpışma Önleme Sisteminin (Airborne Collision Avoidance System, ACAS) yanlış uyarıları yer alabilir. Bu durum, pilotlar ve hava trafik kontrolü için artan iş yükü ve bir takım durumsal karmaşıklığa neden olabilir. Birden fazla hayalet uçak enjekte etmek, gözetleme sistemine karşı ezici bir etkiye sahip olabilir. Schafer vd. (2013), 100 hayalet uçağı rastgele konumlarda olacak şekilde enjekte ederek bu durumun mümkün olabileceğini kanıtlamıştır. Toplamda durumsal farkındalığa ve bazı sistem arızalarına yol açmıştır.

### 2.2.3. Mesaj silme (message deletion)

Uçaklardan gönderilen mesajların silinmesi saldırısı, bir saldırganın uçaktan gönderilen meşru ADS-B mesajlarını hedef alarak manipülasyon yapma girişimini ifade eder. Bu saldırıya bir yöntem olarak CRC olarak bölüm 2.1.13'de açıklanmış veri bütünlüğünün kontrolünü yani iletilen verinin tam olduğunun kontrolünü sağlayan hataların miktarının arttırılması mesajın geçersiz hale gelmesine sebep olabilir. Mesaj silme saldırısından kaynaklanan orta düzeyde bir risk vardır. Çünkü bu saldırıyı gerçekleştirmek oldukça zordur ve belirli bir ölçüde zaman senkronizasyonu gerektirir. Bu durum bu saldırının gerçekleştirilme olasılığını düşük yapar. Ayrıca, bu saldırının hava trafik kontrolü ve

gözetleme sistemine etkisi orta düzeydedir. Çünkü bu saldırı gerçekleştirilse bile bir uçağın kontrolörün haritasından kaybolması durumunda, gözetleme sistemi multilaterasyon gibi yedek sistemler tarafından desteklenerek saldırının ciddiyetini azaltır.

### 2.2.4. Mesaj modifiye etme (message modification)

Bir ADS-B mesajının değiştirilmesi çeşitli yöntemlerle gerçekleştirilebilir. Strohmeier (2013) çalışmasında iki farklı mesaj modifiye yönteminden bahsetmektedir. Bunlar gölgeleme (overshadowing) ve bit çevirmedir (bit-flipping). Gölgeleme; standart ADS-B yayın kaynağı tarafından iletilen mesajın belirli kısımlarını değiştirip mesajı çok daha güçlü bir sinyal göndermeyi olarak göndermeyi içerir. Bit çevirme ise mesajın belirli bitlerini ters çevirerek bilgiyi değiştirmeyi sağlar. Schafer ve diğerleri (2013) gölgeleme yaklaşımını kullanarak bir mesaj değiştirme saldırısı da başarıyla gerçekleştirdi. Bir uçağın rotası değiştirilmiş şekilde konum güncellemeleri gönderilerek değiştirildi. ADS-B'nin tek veri kaynağı olduğu yerlerde böyle saldırıların fark edilmesi oldukça zordur. Saldırganın uzaktan uçağı ele geçirip hava araçlarının çarpışmasına neden olabileceği için hava trafik kontrolü üzerinde yüksek etkiye sahiptir. Bu saldırının karmaşıklığı, gerektirdiği sıkı zaman senkronizasyonu ve hassasiyet nedeniyle en yüksektir. Bu nedenle, bu tür bir saldırı orta-yüksek risk olarak değerlendirilir.

### 2.2.5. Karıştırma (jamming)

Tüm Mode-S ADS-B servisini engellemek başka bir güvenlik tehdidi oluşturabilir. ADS-B yayınlarının sağlandığı 1090 MHz frekans bandında yüksek güce sahip bir sinyal gönderilirse ADS-B yayınları kesilebilir. ADS-B sinyallerinin karıştırılması hem yer istasyonunu karıştırarak hem de uçağı karıştırarak sağlanabilir. Yer istasyonunun karıştırılması oldukça düşük maliyete sahip olan SDR'lar ile yapılabilir. Yer istasyonun yakınına giderek yapılacak ADS-B yayın gücünden daha yüksek güçte yayın ile bu sinyaller karıştırılabilir ve potansiyel tehlike yaratılabilir. Hava aracının karıştırılması çok daha zor olsa da yine de mümkündür. Çok yüksek güçte yayın yapılması gerekir. Hava araçlarının ADS-B yayın çıkış güç seviyeleri hava araçlarının tipine ve amacına göre değişebilir. Ufak hava araçları için minimum 75W güç, daha büyük hava araçları için 125W ya da 200 W yayın gücüne ihtiyaç duyarlar (Ying, Mazer, Bernieri, Conti, Bushnell ve Poovendran, 2019).

## 2.3. ADS-B Güvenliği Sağlama Methodları

ADS-B, radar sistemleri gibi diğer havacılık izleme ve yönetme sistemlerine göre düşük maliyete yüksek doğrulukla konum ve diğer bilgilerinin sağlanma avantajına sahiptir. Ancak, herhangi bir güvenlik önlemi barındırmaz. ADS-B'nin daha fazla güvenlik ihtiyacı nedeniyle, bölüm 2.2'de tartışılan saldırı türlerine karşı bir dizi önlemler ve güvenlik protokolleri önerilmiştir. Bu protokollerden bazıları sistem avantajlarını korurken bazıları protokol değişikliği gibi büyük değişiklikler gerektirmektedir.

### 2.3.1. Kriptolama yöntemleri

ADS-B protokolünde gizliliği ve bir tür kimlik doğrulamayı sağlamayı amaçlayan güvenlik çözümleri arasında çeşitli kriptografi yöntemleri bulunmaktadır. Kriptografi, bilgiyi koruyan ve yalnızca yetkili alıcının bilgiye erişimini sağlayan bir yöntemdir. Temelde üç ana türde kriptografi yöntemi incelenebilir. Bunlar simetrik, asimetrik ve karmaşık (hash) şifreleme yöntemleridir. ADS-B'yi şifreli bir protokole dönüştürmek, mesajların güvenliği açısından oldukça önemlidir. İlk olarak, ADS-B'nin uluslararası bir protokol olması, şifreleme yönteminin ADS-B kullanımıyla ilgili mevcut politika ve teknolojik kısıtlamalara uyması gerektiği anlamına gelir. İkinci olarak, ADS-B bant genişliği ve müdahale sınırlamalarına tabidir. Sistem tarafından desteklenebilen maksimum uçak sayısı, müdahale edilebilmesi bağlamında sınırlıdır. Şifreleme yöntemlerini içermek için iletişim uzunluğunu artırmak, bu sınırlamaları daha da artırabilir Dahası, ADS-B, "kriptografik olarak güvenilmeyen bir ortamda" çalışır. Bu durum tüm şifreleme donanımı, yazılımı ve anahtarlarının olası kötü niyetli gruplar için erişilebilir hale gelebileceği anlamına gelir (Yang, Zhou, Yao, Lu, Li, Zhang, 2018).

*Simetrik Şifreleme Algoritmaları*, anahtarların kullanım şeklinden ve gönderen ile alıcı arasında paylaşılmasından türetilmiştir. Simetrik şifrelemede tek bir genel anahtar hem şifreleme hem de şifre çözme için kullanılır. Cook (2015), ADS-B'nin şifrelenebilmesi için Biçim Korumalı Şifreleme (Format Preserving Encryption, FPE) yöntemi gibi çeşitli simetrik şifreleme güvenlik önlemleri ortaya koymuştur. Bu, bir mesajı veri formatını değiştirmeden şifreleyen bir şifreleme yöntemidir. Bu biçim korumalı şifreleme, ADS-B protokolünün mesaj formatını korurken şifrelenmiş bir formatta sunulmasına olanak tanımıştır. Simetrik anahtar şifrelemenin avantajı, veri formatının aynı kalabilmesidir.

Ancak, şifreleme anahtarının yönetimi oldukça büyük bir sorundur. Eğer şifre çözme anahtarı sızdırılırsa, şifreleme tehlikeye girer. ADS-B'nin çalıştığı ortam "kriptografik olarak güvenilmeyen" olduğundan, bu durum anahtar yönetimini zorlaştırabilir.

*Asimetrik anahtar şifreleme*, genel-özel anahtar çiftlerini bir altyapı olan Açık Anahtar Altyapısı (Public Key Infrastructure, PKI) üzerinden dağıtan bir şifreleme düzenidir. Burada protokolün her kullanıcısı, kendi kimliği ile eşleştirilmiş genel ve özel anahtar çiftine sahiptir. Bu genel ve özel anahtar, Sertifika Otoritesi (Certificate Authority, CA) tarafından yönetilmelidir. Mesaj gönderici, mesajı genel anahtarla şifreler ve mesaj alıcısı, mesajı kendi özel anahtarıyla şifresini çözümler. Asimetrik şifrelemenin dezavantajları, ADS-B'nin mesaj uzunluklarının anahtar şifrelerini içerecek şekilde arttırılmasının gerektirecek olmasıdır. Ayrıca, bir PKI uygulamak ek maliyetli olabilir. Yang ve diğerleri (2018) ADS-B'yi güvence altına almak için olası bir asimetrik anahtar şifreleme durumu hakkında bilgiler vererek çalışmasında bu durumu tartışmıştır. Asimetrik şifreleme durumunda, tam bir anahtar yönetim altyapısı ve en az 448 bitlik anahtar imzaları gerektiğini belirtir. Bu, standart bir 1090ES ADS-B mesajının uzunluğunun dört katıdır. Asimetrik şifreleme kullanıldığında, gönderici iletimden önce alıcıyı bilmelidir. Bu sebeplerden ötürü, ADS-B'nin gerçek zamanlı konum verisi paylaşabilmesindeki olumlu etkilerini azalacaktır.

*Karma (Hash) Teknikleri veya Karma Fonksiyonları (Hashing Function),* belirli bir uzunluktaki giriş verilerini sabit bir uzunluktaki bir çıkış değerine dönüştüren fonksiyon türleridir. Bir kriptografik hash fonksiyonu, tersine çevrilemez ve benzersiz olmalıdır. Yani, orijinal veriyi hash değerinden geri elde etmek mümkün olmamalı ve her farklı giriş verisi için benzersiz bir hash değeri üretilmelidir. Bazı kriptografik güvenlik çözümleri, özellikle blok zinciri teknolojisi, bu karma fonksiyonlarından yararlanır. Blok zinciri, bir veritabanını veya ağı oluşturan tüm işlemlerin dağıtılmış bir kaydını temsil eder. Bu çerçevede, ağın durumuna dair bilgileri içeren bloklar bir zincir oluşturur. Her blok, içinde bulunan verilerin yanı sıra önceki bloğun hash değerini de içerir, bu da blokları birbiriyle zincirleme bir şekilde bağlar. Bu yapı, blok zinciri içindeki her varlığın kendi veri kopyasını saklamasına olanak tanır. Sonuç olarak, zincir dağıtıldığında, blok zinciri veritabanı güvenliği sağlamak için kritik bir role sahip olur. Bu teknolojinin ADS-B'nin güvenlik sorunlarına yönelik potansiyel bir çözüm olarak uygulanması mümkündür (Strohmeier, 2013). Bu teknoloji, ADS-B güvenlik sorunlarına bir çözüm sağlamak için

uygulanabilmekle birlikte ADS-B teknolojisinde ciddi altyapı değişikliği ve maliyet gerektirmektedir.

### 2.3.2. Kalman Filtrelemesi

Rudolf Kalman tarafından bulunan Kalman Filtresi, günümüzde kullanılan en önemli durum kestirme tekniklerindendir. Bu filtrelemenin temel fikri, ölçülen ve öngörülen durum arasında ağırlıklı bir ortalama hesaplamaktır. Bu ağırlık, ölçümün belirsizlik düzeyi ve gürültü miktarına bağlıdır. Havacılıkta GPS sistemlerinde kullanılmaktadır. Kalman filtreleri ile tutarlı ve tutarsız ADS-B verileri arasında ayrım yapmak mümkündür. Kovell, Mellish ve Newman (2012), bu konuda bir güvenlik katmanı sağlanabileceğinden bahseder. Ancak, yöntemin halen kolayca aldatılabileceğini, yeteri kadar büyük bir güvenlik katmanı eklenmediğini de belirtir. Öte yandan Leonardi ve Sirbu (2021), çalışmasında TDOA'ın da yardımıyla, yapılabilecek GPS sahteciliğini (Spoofing) ve GPS karıştırmasını (jammer faaliyetleri) yüksek doğrulukla tahmin edebileceğini belirtmektedir. Ancak, ADS-B'ye yönelik yürütülecek diğer tür saldırılar hakkında herhangi bir faydadan bahsetmez.

### 2.3.3. Yayılı Spektrum (Spread Spectrum)

ADS-B protokolünde erişilebilirliği sağlamayı ve bazı durumlarda kimlik doğrulamayı amaçlayan teknolojiler arasında yayılı spektrum teknolojileri bulunmaktadır. Bu teknoloji daha çok bölüm 2.2.1'de bahsedilen kolay dinlenebilme ve bölüm 2.2.5'te bahsedilen karıştırma faaliyetlerine karşı kullanılabilir (Zhijun ve diğerleri, 2017). Doğrudan dizili yayılı spektrum (direct sequence spread spektrum, DSSS) ve frekans atlamalı yayılı spektrum (frequency hopping spread spektrum- FHSS) olarak adlandırılan 2 farklı yayılı spektrum teknolojisi vardır. Bu yöntemleri kullanabilmek için hem verici hem de alıcı önceden paylaşılmış bir yayılım koduna veya atlama desenine erişime sahip olmalıdır. Bu nedenle, yayılım kodu veya atlama deseni hakkında erişimi veya bilgisi olmayan birinin iletişimi takip etmesi veya dinlemesi zordur. Her iki tarafın da kodu bilmeleri gerektiği için, kriptografik şemalara benzer şekilde, yayılı spektrum da sistemde kod dağıtımı ve yönetiminin zorluğuyla karşı karşıya kalınabilir. Strasser, Pöpper, Capkun ve Cagalj (2008) ve Pöpper, Strasser ve Capkun (2009) çalışmalarında yayılım kodu ve atlama deseni kullanmadan spread spektrum tekniği kullanabileceğini çalışmalarında göstermişlerdir. Ancak bu yöntemlerin ADS-B altyapısıyla uyumlu olmayışı ve sisteme

önemli değişiklikler getirecek olması hasebiyle implementasyonu oldukça zor görülüp daha az uygulanabilir durumdadır.

### 2.3.4. Mesafe Sınırlayıcı (Distance Bounding)

Mesafe sınırlama, elektromanyetik dalgaların en fazla ışık hızı $c$ ile seyahat edebileceği gerçeğine dayanan bir konum doğrulama yöntemidir. Bu yöntemin arkasındaki fikir, gönderilen ve yanıt mesajlarının gidiş dönüş süresi ve bir miktar işlem süresi ile mesafenin hesaplanmasına dayanır. Bu ek mesafe bilgisi, ADS-B ile iddia edilen GPS konumunun doğruluğunu doğrulamak için kullanılabilir. Kim, Jo, Lee (2017) çalışmasında ADS-B güvenliğinin sağlanabilmesi için mesafe sınırlayıcı önermiştir. Bu işlem protokol değişikliğine neden olacağı için implementasyonu fazla kaynak gerektirmekte olup uygun bulunmamıştır.

### 2.3.5. Radyo Frekans Parmak İzi (RFF)

Bu tez çalışmasının ana konusu olan bu yöntem Bölüm 3'de anlatılmıştır.

## 2.4. ADS-B Güvenliği Hakkında Literatürdeki Çalışmalar

Reisman (2019), ADS-B'yi doğrulamak ve güvenli hale getirmek için blok zincirinden esinlenmiş bir Genel Anahtar Altyapısı (Public Key Infrastructure, PKI) çerçevesi önermektedir. Önerisinde, mevcut Ulusal Hava Sahası Sisteminde (National Aviation System – NAS) radar tabanlı hizmetlerin sunduğu uçak gizliliği düzeylerini koruyan hatta aşan ADS-B havacılık gözetleme hizmetlerini desteklemektedir.

Amin, Clark, Offutt ve Serenko (2014), ADS-B sinyalinin karıştırılmasını veya sahte mesaj (Mesaj Enjeksiyonu) iletimini önleyebilen güvenli bir sistem tasarlamışlardır. ADS-B iletimi sırasında sahte mesaj saldırılarını tespit etmek ve önlemek için farklı teknikler kullanarak bunları karşılaştırıp en iyisini seçmeye çalışmışlardır. İlk kullanılan teknik, mesajların sonuna bir karma algoritması ekleyip bunu mesajın kaynağını ayırt edebilmek için kullanılmıştır. Araştırmacılar ayrıca mesaj gizliliği, inkâr edilemezlik, kimlik doğrulama ve bütünlüğünü garanti etmek için simetrik ve asimetrik şifreleme de kullanmışlardır. Simetrik şifrelemede sadece paylaşılan genel anahtarları kullanırken, asimetrik şifreleme hem genel hem de özel anahtarları kullanır. Araştırmacılar, sahte mesaj

saldırılarından kaçınmak ve ekonomik etkenlerden en az etkilenmek için en iyi tekniğin simetrik şifreleme olduğunu önermektedirler.

Hableel, Baek, Byon ve Wong (2015), yer istasyonlarının kontrolörleri için özel anahtar oluşturan Aşamalı Kimlik Tabanlı Şifreleme (Staged Identity Based Encryption, SIBE) şifreleme şemasını önermektedirler. Araştırmacılar, SIBE şemasını Hibrit Kimlik Tabanlı Şifreleme'nin (Hibrit Identity-Based Encryption, HIBE) genişletilmiş bir versiyonu olarak tanımlamaktadır. SIBE'nin amacı, simetrik şifreleme düzenini etkili bir şekilde kullanarak yoğun Kimlik Tabanlı Şifreleme (Identity-Based Encryption, IBE) işlemlerini en aza indirgemek ve genel verimliliği artırmaktır. SIBE şemasının ana fikri şudur: Tüm yer kontrolörlerinin benzersiz tanımlayıcılarıyla belirlendiğini ve bu tanımlayıcılardan, ilgili yetkili olan Özel Anahtar Üreteci'nin özel anahtarlarını oluşturduğunu varsaymaktadır. Bir uçak, yer kontrolörünün yönettiği bir hava sahasına girdiğinde, yer kontrolörünün kimliği ile güvenli bir şekilde oluşturulan rastgele bir simetrik anahtarı şifreler. Ardından, seçilen rastgele anahtar altında AES gibi bir simetrik şifreleme düzenini kullanarak sonraki mesajları şifreler. Yer kontrolörü, uçaktan gelen ve rastgele simetrik anahtarın şifrelendiği mesajı aldığında, kendi kimliği ile ilişkilendirilmiş özel anahtarını kullanarak bunu çözer ve böylece uçaktan gelen sonraki şifreli metinlerini çözerek şifreli haberleşmeyi gerçekleştirir.

Alghamdi, Alshhrani ve Hamza (2018), ADS-B mesajları için en uygun olan şifreleme yönteminin SIBE olduğunu savunur. Bu yöntemin yeterli düzeyde güvenli olduğundan bahseder. Bu tekniğin gizlilik, verimlilik ve etkili anahtar yönetimi ile sık şifreleme için yeterince uygun olduğunu belirtir. ADS-B mesajlarına yönelik gelebilecek tehditlere karşı kullanılabilecek mevcut farklı şifreleme tekniklerinden bahsederek SIBE'nin daha uygun olduğundan bahsetmiştir.

# 3. RADYO FREKANS PARMAK İZİ

Radyo Frekansı Parmak İzi (Radio Frequency Fingerprinting, RFF) teknikleri, kablosuz cihazlar için ek bir güvenlik katmanı olarak kullanılmaktadır. Kablosuz cihazlar, radyo devrelerinden kaynaklanan benzersiz RFF tarafından tanımlanabilir ve sınıflandırılabilirler. RF parmak izleri üretici tarafından üretim sırasında analog bileşenlerin (donanım) rastgele kusurlarından kaynaklanarak ortaya çıkmaktadır. Sinyalin göndericisini benzersiz bir şekilde tanımlamak için kullanılabilir. Ayrıca, aynı vericilere ait iki cihazın tam olarak aynı parmak izine sahip olma olasılığı çok düşüktür. RFF birçok farklı cihazın parmak izini sağlamak için kullanılabilir. Uygulama örnekleri arasında uçakları tanımlamak için ADS-B sinyallerinin parmak izi, wi-fi cihazları ve push-to-talk radyo vericileri olabilmektedir (Toonstra ve Kinsner, 1996). RFF çıkarımı sırasında sinyalin taşıdığı bilginin bir önemi bulunmamaktadır. RFF Bölüm 2.2'de belirtilen saldırı yöntemlerini tespit edebilmek veya önlemek için kullanılabilir.

Ali, Uzundurukan ve Kara (2019), Bluetooth (BT) cihazlarından elde edilen geniş kapsamlı verileri RF parmak izi uygulamasında kullanmıştır. Hilbert-Huang Dönüşümü (Hilbert-Huang Transform, HHT), bluetooth cihazı kimliği belirleme için ilk kez RF parmak izleme uygulamasında kullanılmıştır. Çalışmalarında Zaman-Frekans Enerji Dağılımı (Time-Frequency Energy Distrubition, TFED) kullanılmaktadır. 13 farklı sinyal özelliği çıkartmışlardır. Çıkarılan özellikler ile 3 farklı sınıflandırıcı uygulaması sunulmuştur. Farklı Sinyal Gürültü Oranı (Signal to Noise Ratio, SNR) seviyeleri kullanılarak çıkarılan özelliklerin ve sınıflandırıcı performanslarının dayanıklılığı değerlendirilmiştir.

ADS-B havacılığın modernleştirilmesinde temel bir unsur olarak kabul edilmektedir. Ancak birçok araştırmacı ADS-B'nin güvenliği konusunda endişelerini ifade etmiştir. Bu durum ADS-B protokolündeki güvenliği artırmaya yönelik çeşitli çözüm önerileri üzerine birçok araştırmaya yol açmıştır. Bunlar arasında tam şifreleme, veri doğrulama teknikleri ve hatta blok zincir teknolojisi bile bulunmaktadır. Araştırılan tekniklerden biri de radyo frekansı parmak izi sınıflandırmasıdır. Radyo frekansı parmak izi, iletilen ADS-B sinyali üzerinde benzersiz özellikler çıkarılmasının oluşturulabilmektedir. Bu bölüm, RFF hakkında yayınlanan yayınların birçoğu hakkında bilgi vermekle beraber özellik çıkarımı ve IQ verisi hakkında bilgiler verecektir.

## 3.1. Benzersiz özellik çıkarımı (feature extractions)

Radyo frekans parmak izinde özellik çıkarımı, bir kablosuz yayın kaynağından çıkan sinyalinin benzersiz fiziksel özelliklerini ortaya çıkarmak amacıyla yapılır. Çıkartılan özelliklerle sınıflandırma işlemleri yapılabilir. Bu özelliklerden bazıları aşağıda kısaca tanıtılmıştır.

### 3.1.1. Geçici durum temelli özellikler (transient based features)

Sinyalin geçici (transient) bölümlerinden benzersiz özelliklerin çıkartılması işlemine denir. Örneğin, sinyalin başlangıcı, bitişi gibi belirgin geçişler veya büyük değişiklikler gibi durumlarda, sinyal özelliklerini çıkarmak için kullanılan bir yöntemdir. Geçici özellikler, özellikle sinyalin başlangıcını doğru bir şekilde tespit ederek sinyal özelliklerini çıkarmak için oldukça önemlidir (Toonstra ve Kinsner, 1995).

### 3.1.2. Kararlı durum temelli özellikler (steady-state based features)

Bu yöntem, sinyalin sürekli kararlı-durum bölümlerinden sinyale özel özellikleri çıkarmaya odaklanır. Sinyalin genel davranışı ve frekans bileşenleri, bu özelliklere dahildir. Özellikle, sinyalin enerji özellikleri bu kategoriye dahil edilebilir. Örneğin, bir ses dalgası incelendiğinde, sesin kararlı-durum bölümleri genellikle dalganın ortasındaki sabit frekanslı veya sabit genlikli bölümleri temsil eder. Bu bölümler, bir ses sinyalinin karakteristik özelliklerini yansıtabilir.

### 3.1.3. Zaman-frekans analizi

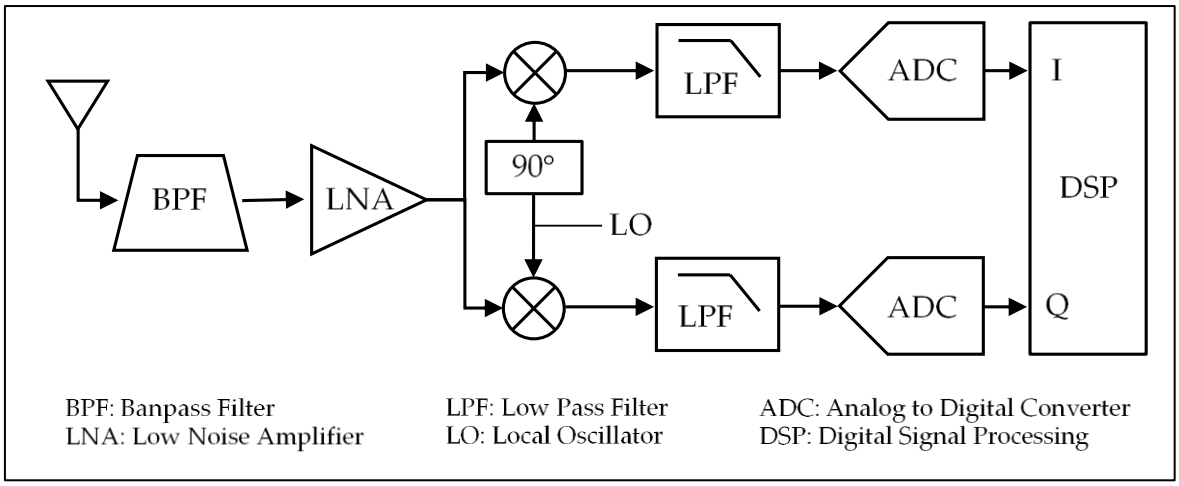
Sinyalin zaman-frekans analizi, belirli bir zaman dilimindeki frekans bileşenlerini ortaya çıkarmak için kullanılır. Hilbert-Huang Transform'u gibi yöntemler bu tür analizlerde sıkça tercih edilir. Sinyalin spektral içeriğini anlamak ve özellikle transients veya frekans değişiklikleri üzerine odaklanmak için kullanılır. Zaman-Frekans analizi ile sinyal özellikleri tespit edilebilir.

### 3.1.4. Modülasyon tabanlı özellikler

Sinyalin modülasyon özellikleri, aynı zamanda taşıdığı bilgileri de kapsar. Örneğin, bir sinyalin taşıdığı verilerin modülasyon türü (örneğin Pulse Position Modulation (PPM), Quadrature Phase Shift Keying (QPSK), Frequency Shift Keying (FSK), Amplitude Modulation (AM) veya Frequency Modulation (FM)) bu özelliklere dâhil edilebilir. Bu modülasyon türlerine göre sinyal özellikleri oluşturulabilir ve bu sinyal özelliklerine göre sınıflandırmalar yapılabilir.

## 3.2. I/Q Verisi

IQ sinyali, bir sinyalin karmaşık zaman alanındaki temsilidir. Faz (In Phase, I) ve kareleme (Quadrature, Q) olmak üzere 2 bileşenden oluşur. Bu iki bileşen, orijinal sinyalin genliği, fazı ve frekansı hakkında bilgiler içerir. Faz bileşeni (I), sinyalin genliğini ve taşıdığı temel bilgileri temsil ederken, kareleme bileşeni (Q) faz kaymasını ve sinyalin özgünlüğünü temsil eder. IQ sinyali, kompleks sayılar olarak ifade edilmekte olup genlik ve faz bilgilerini içerir. IQ sinyalinin kayıt işlemi PlutoSDR ile gerçekleştirilmiş olup tipik SDR mimarisi şekil 3.1'de gösterilmiştir.




Şekil 3.1. Direkt-dönüşüm mimarisiyle tipik SDR örneği

Kayıt edilmiş olan ADS-B sinyalleri (x(t)), faz kanalı $\cos(2\pi f_c t)$ ve kareleme $\sin(2\pi f_c t)$ olarak temsil edilir. Her ikisinde de ADS-B sinyal örneklemesinin gerçekleştiği merkez frekansı ($f_c$) 1090 MHz. dir. Örnekleme işleminden sonra SDR tarafından ortaya çıkan veri şu şeklide ifade edilir;

$$x[n] = I[n] + jQ[n] \tag{3.1}$$

Bu sunulan sinyal, bazı benzersiz ve ayırt edici özellikler içerir ve buna RFF denir. Benzersiz özelliklerin çıkartılmasından önce, sinyallerin bazı yöntemlerle işlenmesi ya da filtreleme tekniklerine tabii tutulmalıdır. En sık kullanılan sinyal özellikleri genlik (amplitude), faz (phase) ve frekans (frequency)'dir. Bu sinyal özelliklerinden genlik $a(n)$;

$$a(n) = \sqrt{I^2(n) + Q^2(n)} \tag{3.2}$$

şeklinde ifade edilir. Faz $\phi(n)$;

$$\phi(n) = \tan^{-1}\left(\frac{Q(n)}{I(n)}\right) \tag{3.3}$$

şeklinde ifade edilir. Frekans $f(n)$;

$$f(n) = \frac{1}{2\pi}\frac{\phi(n) - \phi(n-1)}{\Delta n} \tag{3.4}$$

şeklinde ifade edilmektedir.

### 3.3. Literatürde ADS-B ile RFF Çalışmaları

Ying ve diğerleri (2019) yaptıkları çalışmada, hava aracı ADS-B sahtecilik saldırılarını (Spoofing Attack) 96.66% doğrulukla tespit edebildiğini belirtir. Çalışmasında gerçek ADS-B sinyallerini Evrensel Yazılım Radyo Çevre (Universal Software Radio Peripheral, USRP) kullanarak kaydetmiş, sinyallerin benzersiz özelliği olarak faz kullanmış ve 238 hava aracından 1000'er mesaj ile toplam 238.000 ADS-B mesajı kullanmıştır. SODA adını verdiği Derin Sinir Ağı (Deep Neural Network, DNN) temelli sınıflandırıcı ile sınıflandırma çalışmasını yürütmüştür.

Nicolussi, Tanner ve Wattenhofer (2020) yaptıkları çalışmada, ADS-B yayını yapan hava araçlarına derin öğrenme temelli kimliklendirme sunmaktadır. Bu çalışmada RF yayın kaynaklarının üretimde birebir aynı olamayacağını, sinyal karakteristiklerinin farklı olabileceğinden bahsetmektedir. 274 farklı uçaktan en az 2000 olacak şekilde 3.000.000

mesajı veri seti olarak kullanmıştır. SNR değerlerine dair bir bilgi verilmemiştir. 41.9% doğruluk oranıyla sınıflandırmayı başardığından ve diğer güvenlik sistemleriyle birlikte kullanarak ADS-B mesajlarının tam güvenliğini sağlamada yardımcı olabileceğinden bahsetmektedir. Sinyal özelliği olarak faz örüntüsü, mesaj başlangıç (preamble) fazı ve tüm mesaj üzerindeki faz kullanılmıştır.

Zha, Tian ve Lin (2020) gerçekleştirdikleri çalışmada, ADS-B sinyallerinin RFF yardımıyla sınıflandırılmasını amaçlayan bir çalışma gerçekleştirmiştir. Bu çalışmada, RTL-SDR yardımıyla 5 farklı uçak için 20-30 dB arasında SNR değerine sahip 500'er adet ADS-B sinyalini kaydetmiştlerdir. Bu sinyaller yardımıyla Alexnet Derin Öğrenme tekniği ile 98.6%, Googlenet Derin Öğrenme tekniği ile 97.8% doğrulukla 5 uçağı sınıflandırmayı başarmıştır.

Leonardi ve Gerardi (2020) yaptıkları çalışmada, Mode S kanalında bir sızmanın tespiti için uçaktan iletilen sinyallerden çıkarılan taşıyıcı fazı ve taşıyıcı frekansı özelliklerini kullanan RFF tabanlı bir yöntem önermektedir. Önerilen yöntemin performansı, Raspberry Pi üzerinde çalışan bir SDR ile donatılmış ve Dijital Video Yayıncılığı-Karasal (Digital Video Broadcast-Terrestrial, DVB-T) dongle'ı modifiye edilerek kullanılmıştır. Ayrıca, çok yönlü (omnidirectional) bir ADS-B anteni kullanılarak 2942 uçaktan yaklaşık 45 milyon mesaj toplanarak yapılan bir sınıflandırma değerlendirilmiştir. Değerlendirme, kayar pencere boyutlarının (sliding window) ve k-en yakın komşu (k-nearest neighbors, KNN) algoritmasındaki k parametresinin çeşitli değerleri altında gerçekleştirilmiştir.

Louwen (2022) çalışmasında, Karmaşık Değerli Evrişimli Sinir Ağı (Complex Valued Convolutional Neural Networks, CNN) modeli kullanılarak uçak tanımlama için bir Radyo Frekansı Parmak İzi yöntemi önermektedir. Önerilen modelin performansını değerlendirmek için, 50 uçaktan gelen hem ADS-B hem de VHF Veri Bağlantısı Modu 2 (VHF Data Link Mode 2, VDL2) mesajları RTL-SDR donanımı aracılığıyla birkaç gün boyunca toplanmıştır. Modelin sağlamlığı, çeşitli SNR seviyeleri, donanım benzerlikleri, kanal etkileri ve mesaj enjeksiyonları açısından değerlendirilmiştir. RFF performansı üzerindeki SNR'ın etkilerini test etmek için, 50 uçaktan toplanan mesajlar 10 dB SNR seviyesine getirilmiştir. 10 dB SNR'da önerilen modelin doğruluğunun %44 olduğu bulunmuştur.

I. Agadakos, N. Agadakos, Polakis ve Amer (2020) gerçekleştirdikleri çalışmada, wi-fi ve ADS-B sinyallerinin ham I/Q verilerini kullanarak cihazların benzersiz parmak izlerinin oluşturulması için Tekrarlanan Derin Karmaşık Değerli Ağ (Recurrent Deep Complex-Valued Network, RDCN) önermektedir. Performans değerlendirmesi için, ADS-B sinyalleri, çeşitli SNR seviyelerinde (2 - 5 dB) bir SDR tarafından yakalanmıştır. Deneyler, RDCN ağının tüm SNR seviyelerinde neredeyse %100 doğruluk elde edebildiğini göstermektedir.

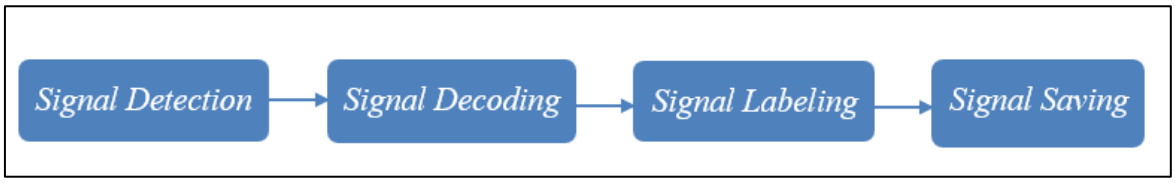
Jian ve diğerleri (2020) gerçekleştirdikleri çalışmalarda, AlexNet'ten esinlenilmiş bir temel model ve Kalıntı Ağ (ResNet) temelli bir ResNet-50-1D modeli, kanalın etkisi, cihaz sayısı, SNR seviyeleri ve veri seti büyüklüğü gibi çeşitli senaryolar altında Radyo Frekans Parmak İzi için kapsamlı bir şekilde incelenmiştir. Modellerin doğruluğu üzerindeki SNR etkileri, 100 cihazdan toplanan 120000 ADS-B iletimini içeren bir veri seti kullanılarak değerlendirilmiştir. Farklı SNR seviyeleri (-13.3 – 15.3 dB) dikkate alınmıştır. En yüksek doğruluk oranı, %92.5 ile temel model tarafından elde edilmiş olup, bu oran ADS-B sinyallerinin ham I/Q verileri düşük SNR (1.9 – -13.3 dB) ile eğitildiğinde ve orta SNR seviyesinde (5 – 2 dB) test edildiğinde bulunmuştur.

Çizelge 3.1. Literatürde bulunan RFF ile ADS-B sinyallerini sınıflandıran çalışmalar

| Ref. | Benzersiz Özellik | Sınıflandırıcı | Yayın Kaynağı Sayısı | SNR | Doğruluk Oranı |
|---|---|---|---|---|---|
| Ying vd. (2019) | Taşıyıcı faz | DNN | 238 | NA | 96,66% |
| Leonardi ve Gerardi (2020) | Taşıyıcı faz ve frekans özellikleri | Sliding Window Size and KNN | 2942 | *NA* | *NA* |
| Zha vd. (2020) | Contour stellar görüntüleri | CNN | 5 | 20 – 30 dB | ~95% |
| Nicolussi vd. (2020) | Başlangıç fazı ve faz örüntüsü | CNN | 274 | *NA* | 41.9% |
| Louwen (2022) | Başlangıç ve bit senkronizasyonu | Complex-valued CNN | 50 | 10 dB | 44% |
| Agadakos vd. (2020) | Ham I/Q verisi | RDCN | 100 | 2-5 dB | ~100% |
| Jian vd. (2020) | Ham I/Q verisi | Baseline and ResNet-50-1D | 100 | -13.3 – 15.3 dB | 92.5% |

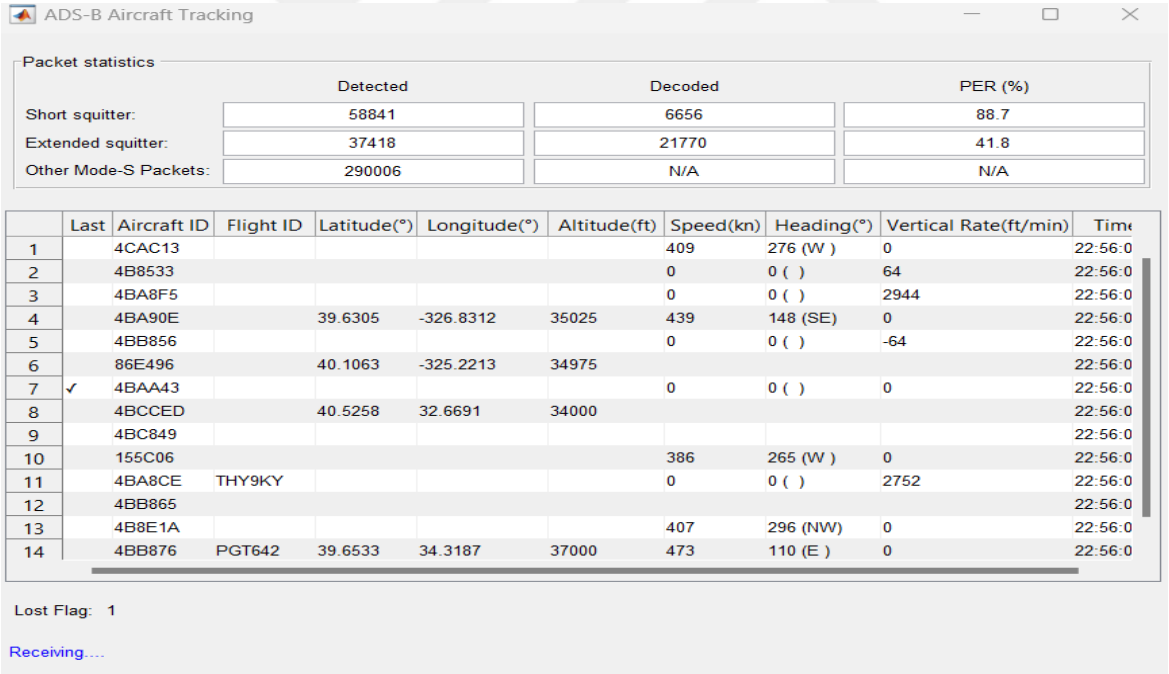
Bu çizelgenin yorumlanması Bölüm 6.1'de tez çalışmasının sonuçlarına yönelik yapılan tartışmada yapılmıştır.

# 4. VERİ TOPLAMA VE FİLTRELEME




Şekil 4.1. ADS-B Sinyali kayıt aşamaları

ADS-B sinyalleri L bandında 1090 MHz frekansında Mode-S yayın kaynağı tarafından yayınlanır. Bu çalışmada 1090 Mhz frekansını dinleyebilmek için SDR kullanılmıştır. Adalm Pluto SDR (PlutoSDR) Analog Devices tarafından geliştirilmiş küçük boyutlu ve düşük maliyetli bir yazılım tabanlı radyo cihazıdır. Bu cihaz, 325 MHz ile 3.8 GHz arasındaki frekans aralığında çalışabilir. Aynı anda alıcı (Rx) ve verici (Tx) özelliklerine sahiptir.



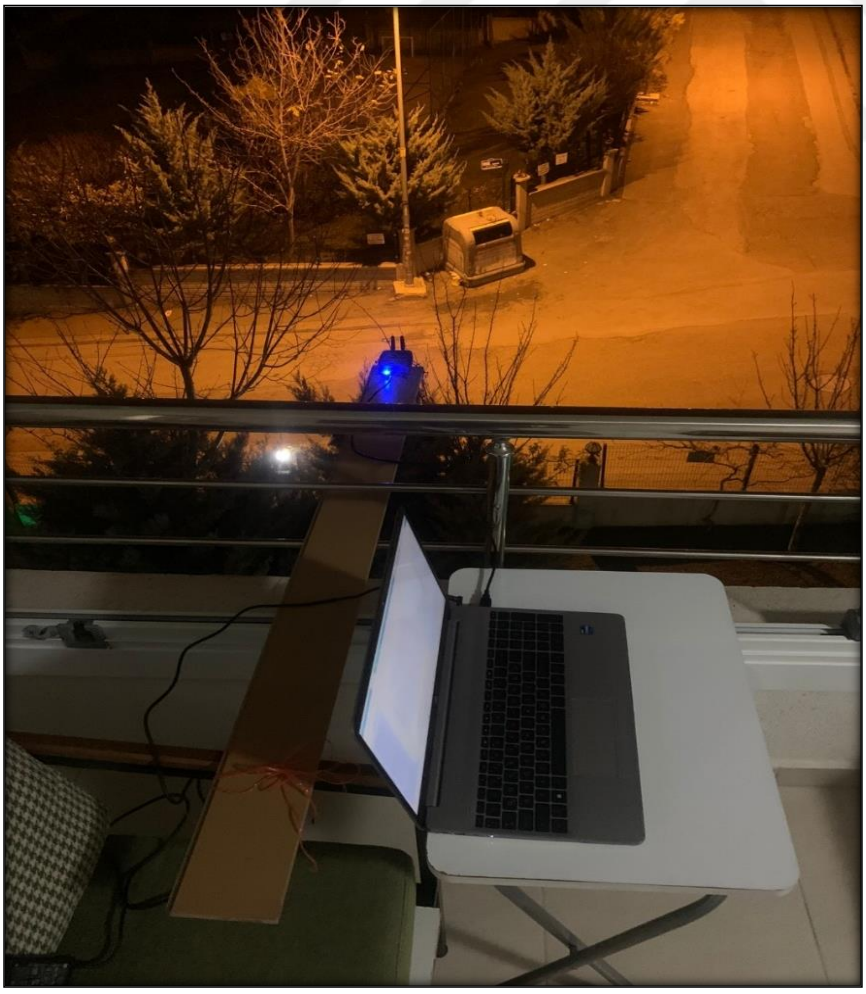

Şekil 4.2. MATLAB'da SDR ile gerçek zamanlı ADS-B mesajları takip uygulamasına ait arayüz

Sinyal kaydı, çözümlenmesi, etiketlenmesi ve filtrelenmesi işlemlerinin tamamı MATLAB üzerinde gerçekleştirilmiştir. Sinyallerin kaydı için kullanılacak yazılımda gerçek zamanlı hava araçlarının yer, konum, hız vb. bilgileri takip edilebilmiş, bunların konumları haritada MATLAB uygulaması vasıtasıyla gösterilebilmiştir. Aynı zamanda bu hava araçlarına ait

mesajlar kayıt altına alınmış, istatistiksel veriler elde edilmiştir. Bu bölümde toplanan verilerin filtrelenmesi, normalizasyon işlemleri ve ADS-B sinyallerinin benzersiz özelliklerinin çıkarılması hakkında bilgiler verilecektir.

## 4.1. Verilerin Toplanması

Veri kayıt sürecinde 988 farklı ICAO kodlu uçaktan toplam ~150000 sinyal kayıt edilmiştir. Bu sinyaller kayıt edilirken ICAO kodu, tarih, saat, saniye ve salise sıralamasıyla kaydedilmiştir. Toplam kayıt süresi yaklaşık 2 ay sürmüş olup her bir kayıt 2026KB boyutundadır. Verilerin kaydı esnasında SDR evin balkonundan dışarı sarkıtılmıştır. Bu sayede yüksek binaların oluşturduğu sinyal kesintilerinin önüne geçilmiştir. Kablo kaynaklı RF kayıplarını ve ekstra gürültüyü minimuma indirmek amacıyla yağmursuz havalarda SDR'ın tamamı balkon dışına sarkıtılarak antenlerin uzatılmasıyla yaşanabilecek RF kayıpları ve gürültüsü önlenmiştir. Kayıt yeri Ankara'dır.



Şekil 4.3. Sinyal kaydının gerçekleştiği alan

Kayıt işlemi MATLAB ortamında gerçekleştirilmiştir. Bu süreç için "Communication Toolbox" ve "Communications Toolbox Support Package for Analog Devices® ADALM-PLUTO Radio software Add-On" eklentileri kurulmuştur. Bu eklentiler PlutoSDR'ı etkin bir şekilde çalıştırabilmemizi sağlamış ve gerekli yazılım düzenlemeleri ile düzenli olarak sinyal kaydedebilmemize olanak tanımıştır. 1090 Mhz'de 1 Mbit/s data rate ile 12 Mhz Sample Rate olacak şekilde gerekli ayarlamalar ile kayıt süreci gerçekleştirilmiştir. Kayıt işlemi ve testler, HP 250 G9 model bilgisayar üzerinde yapılmıştır. Bu bilgisayar Intel i7-1255u işlemci, 24GB RAM ve Iris Xe Graphics ekran kartına sahiptir.

Elde edilen kayıtlardan rastgele 8 farklı uçak seçilerek her bir uçağa ait 435 adet olmak üzere toplam 3480 adet ADS-B sinyaline sahip bir veri seti oluşturulmuştur. Bu sinyaller 4.2.4'de belirtilen filtreleme işlemlerine, 4.3'de belirtilen normalizasyon işlemlerine ve 4.4'da belirtilen özellik çıkarımı işlemlerine tabii tutulmuştur.

## 4.2. Temel Filtreleme Yöntemleri

Sinyal işlemede filtreleme, ham verilerden istenmeyen bileşenleri çıkarmak veya belirli sinyal özelliklerini vurgulamak için kullanılır. Filtreleme yöntemleri genellikle gürültüyü azaltmak, sinyal bütünlüğünü korumak ve analiz için sinyali daha kullanılabilir hale getirmek amacıyla kullanılır. Bu yöntemler arasında temel olarak Hareketli Ortalama Filtresi (Moving Average Filter, MAF), Alçak Geçiren Filtre (Low-Pass Filter, LPF), Yüksek Geçiren Filtre (High-Pass Filter, HPF), Bant Geçiren Filtre (Band-Pass Filter, BPF) gibi filtre tipleri bulunur. Her bir filtre tipi, sinyalin belirli frekans bileşenlerini hedef alarak sinyalin analizinde veya işlenmesinde kullanılır. Bu filtreler, sinyal işlemeden haberleşme sistemlerine, akustik analizden biyomedikal sinyal işlemeye kadar geniş bir uygulama yelpazesinde kullanılır. Etkili bir filtreleme süreci, sinyalin doğruluğunu ve yararlılığını artırırken, istenmeyen gürültü ve distorsiyonları minimuma indirger.

### 4.2.1. Alçak Geçiren Filtre

Alçak Geçiren Filtre, belirli bir kesim frekansının altındaki frekans bileşenlerini geçirirken bu frekanstan daha yüksek frekanslardaki bileşenleri engelleyen bir filtre türüdür. Bu tür filtreler, yüksek frekanslı gürültü ve istenmeyen sinyal bileşenlerini etkili bir şekilde azaltabilir. Alçak geçiren filtreler, sinyal işlemede temel bir araç olup analog ve dijital

formda tasarlanabilirler. Bu filtreler sinyalin temel bileşenlerini korurken istenmeyen yüksek frekanslı parazitleri etkili bir şekilde azaltır.

### 4.2.2. Yüksek Geçiren Filtre

Yüksek Geçiren Filtre, adından da anlaşılacağı gibi belirli bir kesim frekansının üzerindeki frekansları geçirirken, altındaki frekansları engeller. Bu filtre tipi, düşük frekanslı gürültü ve istenmeyen sinyal bileşenlerini filtrelemek için kullanılır. Yüksek geçiren filtreler sinyal işlemede özellikle basit DC bileşenlerini veya düşük frekanslı arka plan gürültülerini çıkarmak için kullanılır. Bu filtreler, genellikle sinyal analizi ve işleme uygulamalarında, sinyalin yüksek frekanslı bileşenlerini vurgulamak ve analiz etmek için tercih edilir. Yüksek geçiren filtreler, sinyalin temel karakterini değiştirebilir.

### 4.2.3. Bant Geçiren Filtre

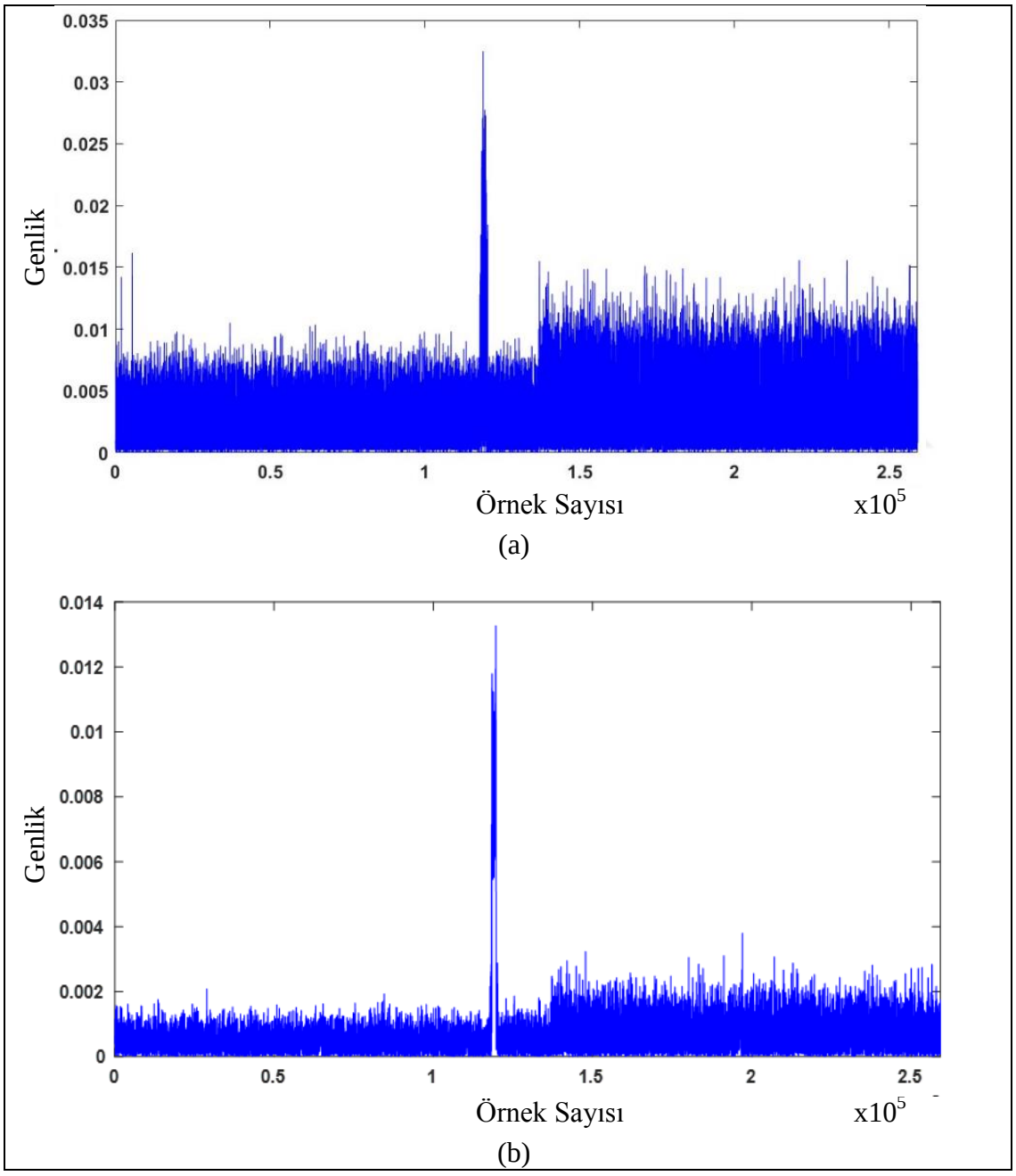
Bant Geçiren Filtre, belirli bir frekans aralığındaki sinyalleri geçiren bu aralığın dışındaki frekansları ise engelleyen bir filtredir. Bu tip filtreler, genellikle belirli bir frekans bandındaki sinyal bileşenlerini izole etmek ve diğer tüm bileşenleri reddetmek için kullanılır. Bant geçiren filtreler haberleşme sistemlerinde, sinyal işlemede ve elektronik müzik üretiminde yaygın olarak kullanılır.

### 4.2.4. Hareketli Ortalama Filtre

Hareketli Ortalama Filtre, zaman serisi verilerindeki gürültüyü azaltmak ve veri setinin genel eğilimini belirlemek için kullanılan basit aynı zamanda etkili bir yöntemdir. Bu filtre, belirli bir pencere büyüklüğüne sahip ardışık veri noktalarının ortalamasını alarak çalışır. Pencere, sinyal üzerinde kaydırılarak her noktada yeni bir ortalama hesaplanır. Bu işlem, sinyalden kısa süreli dalgalanmaları ve rastgele gürültüleri filtreleyerek daha düzgün ve temsil edici bir sinyal elde edilmesini sağlar. Hareketli ortalama filtre, özellikle düşük frekanslı gürültünün azaltılması ve trend analizlerinde oldukça etkilidir. Ancak, bu yöntem sinyalin bazı önemli bileşenlerini de yumuşatabilir veya geciktirebilir. Filtre pencere boyutunun dikkatli bir şekilde seçilmesi gerekir. Matematiksel olarak

$$\bar{x}[j] = \frac{1}{NP} \sum_{k=0}^{NP-1} x[j+k] \tag{4.1}$$

şeklinde ifade edilir (Smith, 2003:277). Burada $\bar{x}[\,]$ filtreleme sonucu oluşan sinyal, $x[\,]$ SDR ile kayıt edilmiş IQ giriş sinyali, $NP$ ise hareketli ortalama filtresindeki örnek sayısını temsil eder. Bu işlemlere göre giriş sinyali ($x[\,]$) ve filtrelenme sonucu oluşna çıkış sinyali ($\bar{x}[\,]$) e dair örnekler aşağıdaki görselde gösterilmişlerdir.




Şekil 4.4.(a) Filtreleme öncesi kayıt edilmiş örnek ADS-B sinyali; (b) Filtreleme sonrası örnek sinyal

Şekil 4.4.'te görüleceği üzere örnekteki sinyalin SNR değeri filtreleme sonrası oldukça yükselmiştir. Bu filtreleme ile sinyal bölgesi gürültü altında kaybolan yani SNR değeri oldukça düşük sinyallerin sinyal bölgesi tespiti yapılabilir. Bu sayede veri kısmının neresi olduğu anlaşılabilir.

Hareketli ortalama filtresi MATLAB ortamında *movmean(x)* ile ifade edilerek kullanılır. Burada $x$ giriş sinyalini temsil eder. Bu fonksiyon, belirli bir pencere boyutuna göre ardışık veri noktalarının ortalamasını alır ve zaman serisindeki kısa süreli dalgalanmaları ve gürültüyü azaltmaya yardımcı olur.

### 4.3. Normalizasyon İşlemleri

Toplanan sinyal verilerinin özellik çıkarımı aşamasına geçmeden önce verilerin normalize edilmesi gerekir. Normalizasyon işlemi farklı ölçeklere veya aralıklara sahip veri noktalarını ortak bir ölçeğe getirme sürecidir. Bu işlem ile veriler arasındaki ilişkiler korunurken, farklı büyüklüklerdeki veriler karşılaştırılabilir hale getirir. Makine öğrenimi algoritmalarının başarısı, sınıflandırma probleminin genelleştirilmiş bir tahmin modelini elde etmek için kullanılan verilerin kalitesine bağlıdır. Veri kalitesinin ve makine öğrenmesi algoritmalarının performansının iyileştirilmesi için verilerin normalleştirilmesi oldukça önemlidir. D. Singh ve B. Singh (2020) çalışmasında, normalizasyon işleminin istatistiksel özelliklerinin nasıl kullanıldığına göre kategorize edileceğini belirtmiştir. Bu normalizasyon tiplerini;

- Ortalama ve standart sapma temelli normalizasyon işlemleri,
- Minimum ve maximum değerler temelli normalizasyon işlemleri,
- Ondalık ölçekleme normalizasyonu (Decimal Scaling Normalization, DSN),
- Medyan ve medyan mutlak sapma normalizasyonu (Median and Median Absolute Deviation Normalization, MMADN),
- Tahn temelli normalizasyon (Tahn Based Normalization, TBN),
- Sigmoidal normalizasyon

olarak 6 farklı kategoriye ayırmıştır. Bu normalizasyon tiplerinde en yaygın kullanılan 2 yöntemden bahsedeceğim. *Min-Max Normalizasyonu*, Minimum ve Maksimum Değerler Temelli Normalizasyon tipine dahildir. Bu normalizasyon yöntemi veri setindeki değerleri

belirli bir aralığa, genellikle 0 ile 1 arasına ölçeklendirmek için kullanılan bir yöntemdir. Veri setindeki her bir değeri veri setinin minimum ve maksimum değerlerine göre dönüştürür. Bu süreç, farklı ölçeklere veya birimlere sahip verileri karşılaştırabilir ve birleştirebilir hale getirir.

$$x'_{i,n} = \frac{x_{i,n} - \min(x_i)}{\max(x_i) - \min(x_i)}(nMax - nMin) + nMin \tag{4.2}$$

Burada istenilen aralığa ölçeklendirilebilen genel formülü verilmiştir. $x'_{i,n}$ orijinal veri iken $\min(x_i)$ve $\max(x_i)$ veri setinin minimum ve maksimum değerleridir. $nMax$ ve $nMin$ ölçeklendirmek istenilen yeni aralığın minimum ve maksimum değerleridir. Min-Max Normalizasyonu'nda genellikle 0 ile 1 arasına ölçeklendirme işlemi yapılır. 0 ile 1 arasında ölçeklendirme işlemi yapılırken sahip olunan denklem sadeleşerek

$$x_{norm} = \frac{(x - x_{min})}{(x_{max} - x_{min})} \tag{4.3}$$

haline dönüşür. Burada, $x$ orijinal veridir.

Bu çalışmada bir diğer yaygın kullanıma sahip olan Ortalama ve Standard Sapma Temelli Normalizasyon İşlemleri tipinde bulunan *Z-Score Normalizasyonu* kullanılmıştır. Çalışmada kayıt edilen IQ formdaki ADS-B sinyalleri Z-Score Normalizasyonuna göre normalize edilerek benzersiz özelliklerinin çıkarılması işlemine tabi tutulmuştur. Bu normalizasyon işleminde, $n$ adet normalize edilecek sinyal $\bar{x}_n$ mevcuttur. Bunların ortalaması $E$, standart sapması $s$ olacak şekilde normalize edilmiş sinyal $y_n$ ile gösterilir.

$$y_n = \frac{\bar{x}_n - E}{s} \tag{4.4}$$

Burada

$$E = \frac{\sum_{n=1}^{N} \bar{x}_n}{N} \tag{4.5}$$

ve

$$s = \sqrt{\frac{\sum(\bar{x}_n - E)^2}{N-1}} \tag{4.6}$$

Olarak ifade edilir. Sinyal özelliği çıkarım işlemlerine başlamadan önce, sahip olunan veri setinde bulunan ADS-B sinyalleri sırasıyla normalize edilmiştir. Bu normalizasyon işleminde; sinyallerin önce ortalaması bulunup ardından standart sapması hesaplanmıştır. Bu işlemler tamamlandıktan sonra, denklem (4.4) de görüldüğü gibi $y_n$ elde edilebilmesi için gerçek ADS-B sinyalinden ortalaması çıkarılıp standart sapmaya bölünmüştür. Bu aşamanın sonunda elde edilen veri, Z-Score normalizasyonuna göre normalize edilmiş bir sinyale dönüşür. Bu çalışmada bir döngü içerisinde bütün ADS-B sinyalleri teker teker normalize edilmiştir.

### 4.4. ADS-B Sinyal Özelliği Çıkarımı

ADS-B sinyallerinde RFF parmak izi oluşturulurken sinyallerin birçok özelliği kullanılabilir. Bunlar arasında faz özellikleri, genlik özellikleri, frekans özellikleri gibi örnekler mevcuttur. 3.3'de literatürdeki örnekler hakkında bilgi verilmiştir. Literatürdeki çalışmalardan farklı olarak bu çalışmada, ADS-B sinyallerini ayırt edici özellik olarak Güç Spektral Yoğunluğu (Power Spectral Density, PSD) özelliği kullanılmıştır.

Güç spektral yoğunluğu, bir sinyalin frekansta hangi bileşenlere sahip olduğunu ve bu bileşenlerin hangi güç düzeylerine sahip olduğunu gösterir. Bir sinyalin frekans bileşenlerini ve bu bileşenlerin güç dağılımını analiz etmek için kullanılmaktadır.

Suski II, Temple, Mendenhall ve Mills (2008) yürüttükleri çalışmalarında, 802.11a OFDM sinyallerinin RF fingerprinting çalışmalarını Power Spectral Density (PSD) benzersiz özelliğini kullanarak gerçekleştirmiş ve 6db den yüksek SNR'a sahip 3 farklı cihazın sinyallerini 80% e yakın doğrulukla tespit edebilmiştir.

Sarraf (2017) çalışmasında, Welch's Power Spectral Density Estimate özelliklerini kullanarak Elektroensefalografi (Electroencephalography, EEG) sinyallerini K-NN, 3 farklı Destek Vektör Makinası (Support Vector Machine, SVM) ve Yapay Sinir Ağı (Artificial Neural Network, ANN) yardımıyla sınıflandırmaya çalışmış olup 70.5%

doğruluk değeriyle sınıflandırma işlemini başarmıştır. Çalışmasında ifade edildiği üzere Welch PSD tahmini

$$P_{va}^{welch}[d,k] = \frac{1}{NMU}\sum_{n=0}^{M-1}\left|\sum_{l=(Md+n)N}^{(Md+n)N+2L} w[l-(nN+L)]v_a[l]e^{-\frac{2\pi ld}{N}}\right|^2 \tag{4.7}$$

formulüne dayalı olarak yapılır. Burada, $va$ sinyali ve $k$ sinyal spektrumunu göstermektedir $(k = 0, 1, \dots, N-1)$. $w[l]$ simetrik $N$ noktalı bir pencere fonksiyonudur. $M$, her biri $N$ uzunluğunda olan ardışık örtüşme bulunmayan segmentlerin sayısını ifade eder. $U$, $w$ penceresi için normalizasyon faktörü olup

$$U = \frac{1}{N}\sum_{l=-L}^{L} w^2[l] \tag{4.8}$$

denklemi kullanılarak elde edilir. $d$, hesaplamaların yapılacağı veri aralığının başlangıç noktasını gösterir. $L$, veri segmentlerinin uzunluğunu gösterir.

# 5. SINIFLANDIRMA ÇALIŞMALARI

Günümüzde, teknolojinin hızla gelişen alanlarından biri olan Makine Öğrenmesi (Machine Learning, ML) büyük ilerlemeler kaydetmiştir. Veri analizi, otomatik karar alma süreçleri ve öngörücü modelleme gibi çeşitli uygulamalarda önemli bir rol oynayan makine öğrenimi, giderek daha karmaşık problemleri çözebilen modeller ve algoritmalar geliştirmeye olanak tanımıştır. Özellikle, özelleştirilmiş makine öğrenimi teknikleri, sistemlerin karmaşık gizli özelliklerini öğrenerek geleneksel yöntemlere göre daha iyi performans sergileyebilmektedir. Makine öğrenimi temelde, giriş verileri (özellikler) ve çıktı değerleri (etiketler) arasındaki karmaşık ilişkileri yakalamak amacıyla gerçek dünya verilerini kullanarak bir ML çözümünü eğitmek için kullanılır.

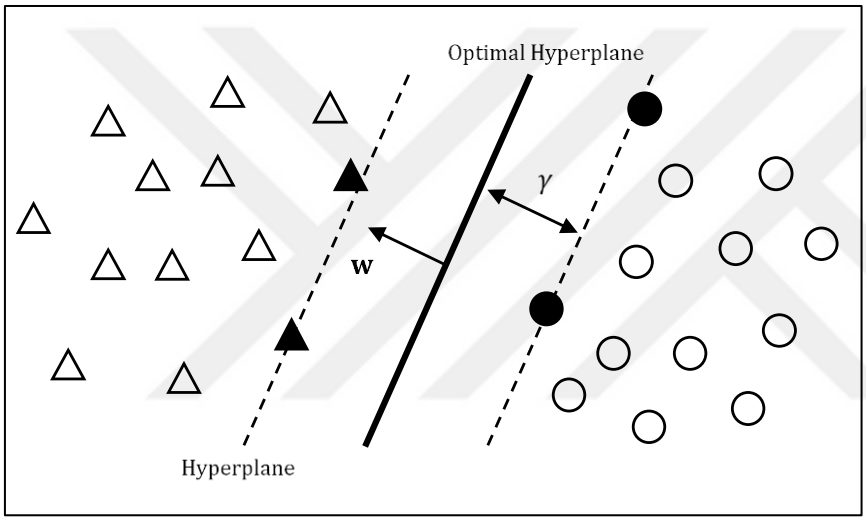
Makine öğrenimi teknikleri, özellikle derin öğrenme (Deep Learning, DL) ve pekiştirmeli öğrenme (Reinforcement Learning, RL) gibi yöntemler, genellikle devasa miktarda ve hedeflenen sistemi yeterince tanımlayacak veriler üzerinde yoğun bir eğitim ve test sürecinden geçmek zorundadır. Bu süreç, çalışan bir modelin doğru bir şekilde oluşturulmasını sağlayarak eğitilen ve test edilen modelin performans analizine imkan verir. Ancak, bu yöntemler geleneksel makine öğrenimi tekniklerine kıyasla önemli ölçüde daha yüksek hesaplama kaynakları gerektirir. Bu nedenle, göreceli olarak küçük veri miktarları üzerinde eğitim yapmak için geleneksel makine öğrenimi tekniklerini kullanmak makul bir seçenek olabilir. Literatürde, Destek Vektör Makinaları güçlü düzenlileştirme özellikleri nedeniyle en başarılı geleneksel makine öğrenimi tekniklerinden biri olarak kabul edilir. Bu bağlamda, ADS-B sinyallerinin sınıflandırılması için SVM tekniğinin kullanılmasına karar verilmiştir.

## 5.1. Destek Vektör Makinaları (SVM)

SVM'lerin temellerini açıklamak için en erken örüntü tanıma sistemlerine (Pattern Recognation System) geri dönülmesi gerekmektedir (Bottou ve Lin, 2007). Tipik bir örüntü tanıma sisteminde, bir örüntü $\mathbf{x}$, örüntünün bir özellik vektörü $\Phi = (\mathbf{x})$'e dönüştürülmesi ve

$$\hat{y}(\mathbf{x}) = \mathbf{w}^T \Phi(\mathbf{x}) + b \tag{5.1}$$

şeklinde ifade edilen bir ayrım fonksiyonunun işaretinin alınması yoluyla $y = \pm 1$ sınıfına atanır. Burada özellik uzayındaki bir karar sınırı $\hat{y}(\mathbf{x}) = 0$ hiper düzlemi tarafından belirlenir. Yan parametresi $b$ ve parametre $\mathbf{w}$, $(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \cdots, (\mathbf{x}_n, y_n)$ şeklindeki bir eğitim veri seti üzerinde gerçekleştirilen bir öğrenme süreci sonucunda belirlenir. Eğitim seti doğrusal olarak ayrılabilir olduğunda hiperdüzlemleri ayırmak için birçok farklı yol izlenebilir. Bu sebeple burada, hiperdüzlem ile en yakın örnekler arasındaki marjın (γ) maksimum yapılması için optimum bir hiperdüzlem seçilmelidir. Hiperdüzleme en yakın destek vektörleri tarafından belirlenen optimum hiperdüzlemin konumu Şekil 5.1'de gösterilmiştir.




Şekil 5.1. Üçgen ve daire örneklerini (verileri) en yüksek marj ile optimal bir hiper düzlem kullanarak ayırma. Hiper düzleme en yakın olan destek vektörleri, dolu üçgenler ve daireler ile gösterilmiştir.

Marjın maksimum yapılması için optimizasyon problemi aşağıdaki gibi tanımlanabilir:

$$\min \mathcal{P}(\mathbf{w}, b) = \frac{1}{2}\mathbf{w}^2$$
$$\text{subject to } \forall_i \; y_i(\mathbf{w}^T \Phi(\mathbf{x}_i) + b) \geq 1 \tag{5.2}$$

Bu denklem Lagrangian Duallik teorisi kullanarak

$$\max \mathcal{D}(\boldsymbol{\alpha}) = \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{n} y_i \alpha_i y_j \alpha_j \Phi(\mathbf{x}_i)^T \Phi(\mathbf{x}_j)$$
$$\text{subject to } \forall_i \; \alpha_i \geq 1 \text{ ve } \sum_i y_i \alpha_i = 0 \tag{5.3}$$

şeklinde sadeleştirilebilir (Giannessi, 2007).

Daha sonra, optimal hiperdüzlemin yönü ($\mathbf{w}^*$), (5.2)'de verilen optimizasyon probleminin bir çözümü olan ($\alpha^*$) kullanılarak

$$\mathbf{w}^* = \sum_{i=1}^{n} \alpha_i^* y_i \Phi(\mathbf{x}_i) \tag{5.4}$$

olarak belirlenir. Buradan, (5.1)'de verilen ayrım fonksiyonu

$$\hat{y}(\mathbf{x}) = \sum_{i=1}^{n} \alpha_i^* y_i K(\mathbf{x}, \mathbf{x}_i) + b \tag{5.5}$$

şeklinde yeniden yazılabilir. Burada, $K(\mathbf{x}, \mathbf{x}_i)$ veri noktalarını doğrusal bir hiperdüzlem uydurulabilecek şekilde yayan bir kernel fonksiyonunu ifade eder. An-na, Yue, Yun-tao ve Yun-lu (2010) çalışmasında, literatürde yaygın olarak kullanılan kernel fonksiyonlarını 6 gruba toplamıştır. Bunlar doğrusal (linear), polinom (polynomial), ve dairesel tabanlı fonksiyon (radial basis function, RBF), Sigmoid kernel fonksiyonu, Fourier kernel fonksiyonu ve B-spline kernel fonksiyonudur. Bu çalışmada doğrusal, polinom ve dairesel tabanlı kernel fonksiyonları SVM sınıflandırmasında kullanılmıştır.

*Doğrusal kernel fonksiyonu*, verilerin doğrusal olarak ayrılabildiği durumlar için idealdir. Veriler 2 veya daha fazla sınıfa bir doğru veya hiperdüzlem kullanarak ayrılabiliyorsa kullanımı mümkündür. Doğrusal kernel fonksiyonu iki vektörün nokta çarpımı (inner product) olarak tanımlanır. Doğrusal kernel fonksiyonu genellikle

$$K(\mathbf{x}_i, \mathbf{x}) = \mathbf{x}_i \cdot \mathbf{x} \tag{5.6}$$

şeklinde ifade edilir.

*Polinom kernel fonksiyonu*, doğrusal olmayan verileri polinom derecesine göre göre ayrıştırmak için kullanılır. Daha yüksek dereceli polinomlar, daha karmaşık ayrıştırmalar yapabilir, ancak aşırı uyuma (overfitting) neden olabilir. Polinom kernel fonksiyonu

$$K(\mathbf{x}_i, \mathbf{x}) = (\mathbf{x}_i \cdot \mathbf{x} + 1)^d \tag{5.7}$$

şeklinde ifade edilir. Buradaki $d$ önceden tanımlı bir polinom derecesidir.

*Dairesel tabanlı kernel fonksiyonu*, SVM içerisinde kullanıldığında verileri yuvarlak veya elips şeklindeki bölgelerle ayırmaya çalışır. Bu özellikleriyle doğrusal olmayan ilişkiler ile karmaşık veri yapıları ve sınıflandırmalar için tercih edilir. Bu kernel fonksiyonu

$$K(\mathbf{x}_i, \mathbf{x}) = e^{(-\|\mathbf{x}-\mathbf{x}_i\|^2/2\sigma)} \tag{5.8}$$

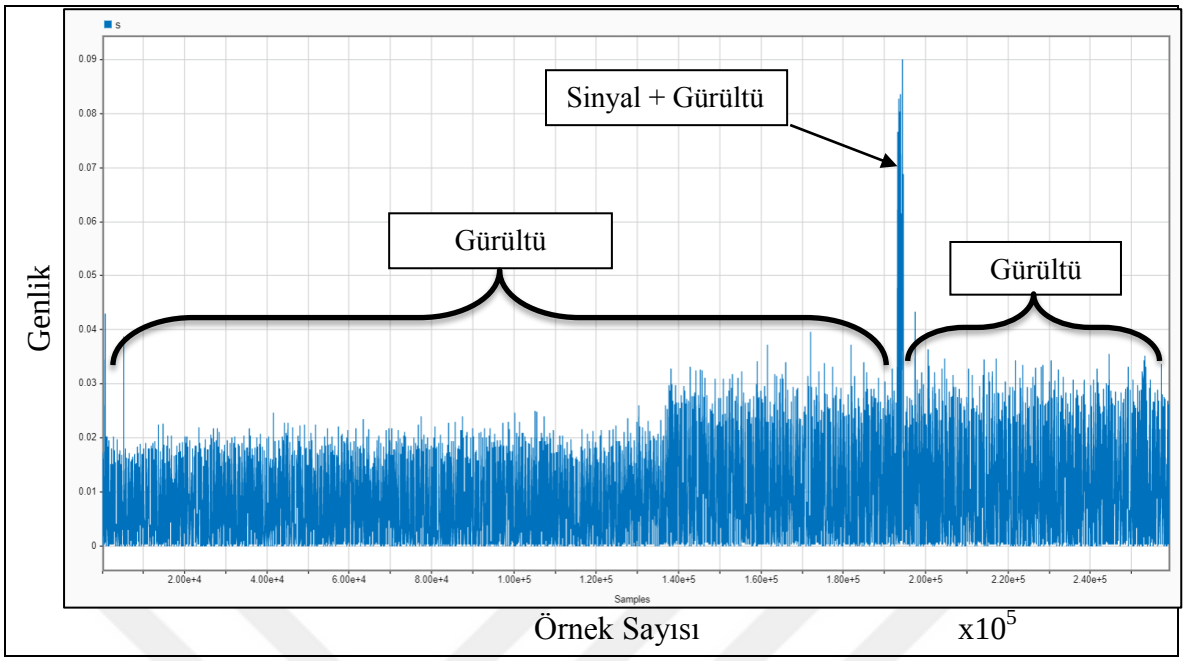
şeklinde ifade edilirler.

## 5.2. Veri Setleri Oluşturulması ve Gürültü Eklenmesi

1090 MHz merkez frekansında ($f_c$) 12 MSPS örneklemesiyle kayıt edilmiş ADS-B sinyallerine dair detaylar 4.1'de sunulmuştur. RFF çalışmalarına etki eden oldukça önemli etkenlerden biriside SNR değeridir. Her bir uçak için 435 adet ADS-B sinyalinden en az 30 dB sinyal-gürültü oranına sahip olacak şekilde farklı SNR değerlerine sahip toplam 3800 adet ADS-B sinyali mevcuttur. Bu çalışmada gerçekleştirilecek sınıflandırma işlemlerinde gürültü performansı da test edilmek istenmiştir. Buna göre 5.2.2'de açıklanan gürültü eklenmek suretiyle veri setleri oluşturulmuştur.

### 5.2.1. Sinyal/gürültü oranı hesaplanması

SNR bir sinyalin gücünün, arka plandaki gürültü gücüne oranını ifade eden bir ölçüttür. SNR, sinyalin kalitesini ve berraklığını değerlendirmek için kullanılır ve genellikle desibel (dB) cinsinden ifade edilir. Şekil 5.2.'de tipik bir ADS-B sinyalinin sinyal ve gürültü bölgeleri gösterilmiştir.




Şekil 5.2. Tipik bir ADS-B sinyalindeki "sinyal" ve "gürültü" bölgeleri

“Sinyal + Gürültü” olarak belirtilen bölge bizim sinyalimizin bilgi içeren kısmıdır. Bu alanda hem sinyal hem gürültü bulunmaktadır. Kalan kısımlarda yalnızca gürültü bulunmaktadır. Bu sebeple SNR oranı

$$SNR(dB) = 10\log_{10}\left(\frac{P_{sinyal}}{P_{gürültü}}\right) \tag{5.9}$$

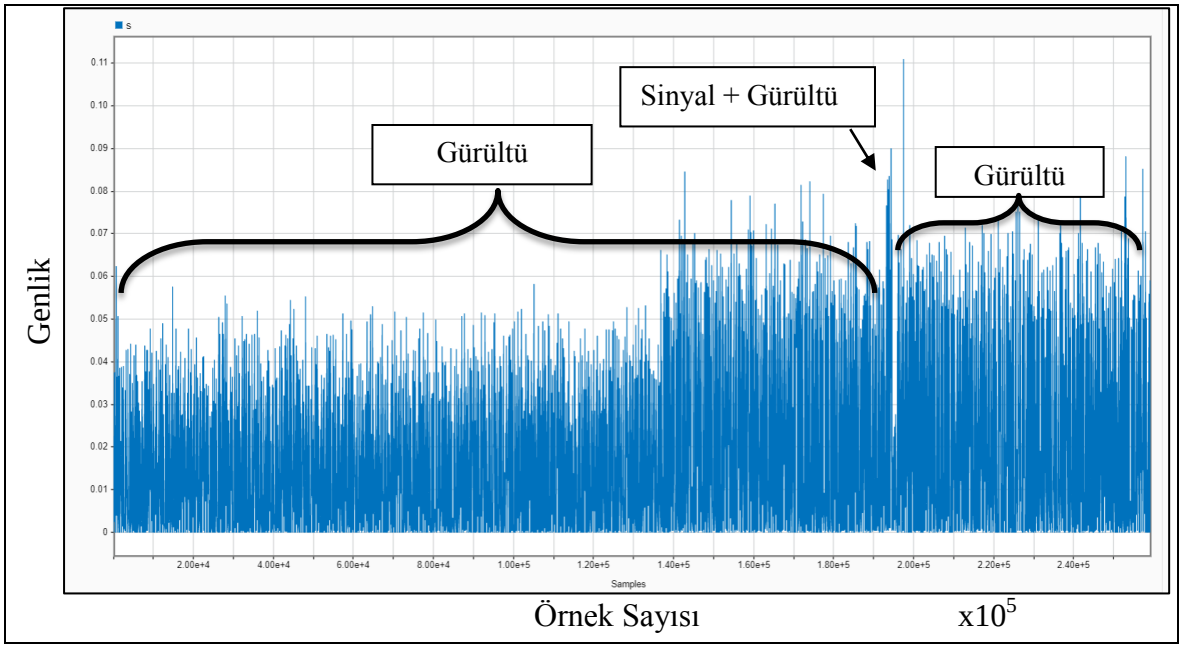
şeklinde hesaplanırken bizim ADS-B sinyallerinizde $P_{sinyal}$ değeri $(P_{sinyal} + P_{gürültü})$’dür. Bu durumda denklemimiz

$$SNR(dB) = 10\log_{10}\left(1 + \frac{P_{sinyal}}{P_{gürültü}}\right) \tag{5.10}$$

Haline gelir ve $SNR(dB)$ değeri formülü ortaya çıkar. Bu formülasyona göre; kayıt edilmiş ADS-B sinyallerinin hepsinin SNR değerleri bulunarak rastgele gürültü eklenerek farklı veri setleri oluşturulmuştur.

### 5.2.2. Gürültü eklenmesi

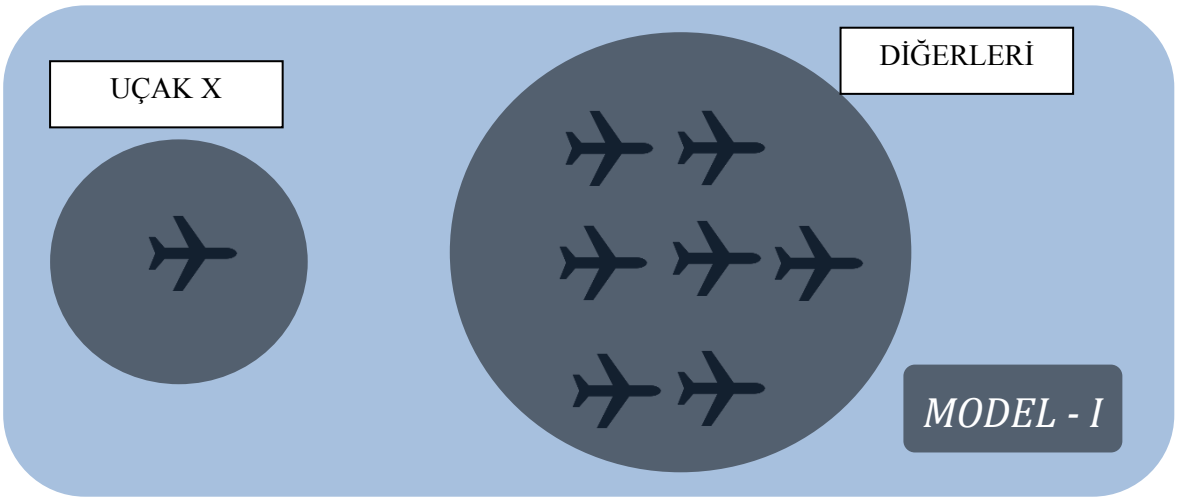
Bu tez çalışmasında sahip olunan en az 30dB SNR değerine sahip 3800 sinyal için rastgele gürültü ekleme işlemleri gerçekleştirilmiştir. Bu işlemlerin sonucunda, 8'er farklı uçağa ait 3800'er adet veri için 5 farklı veri seti oluşturulmuştur. Bu veri setleri 10dB SNR, 15dB SNR, 20dB SNR, 25 dB SNR ve 30 dB SNR olacak şekilde bölümlere ayrılmıştır.




Şekil 5.3. SNR oranı düşük, gürültü eklenmiş ADS-B sinyali

### 5.3. SVM Sınıflandırması

Bölüm 3'de açıklandığı gibi, uçakların yayın kaynaklarının parmak izlerine göre sınıflandırılması benzersiz özellik çıkarımına bağlıdır. Bölüm 4.6'da detaylandırıldığı üzere, her sinyal örneğinin Güç Spektral Yoğunluğu (PSD) uçaklara göre parmak izlerinin oluşturulması için döngü halinde hesaplanmıştır. Daha sonra, PSD'den çıkarılan benzersiz özellikler, kaynak uçağın ilgili ICAO kodu ile etiketlenmiştir. Bölüm 5.1'de tanımlanan SVM yöntemine göre, üç farklı kernel fonksiyonu (lineer, polinom ve RBF) uçakların ikili sınıflandırılması için kullanılmıştır. Şekil 5.4'de gösterildiği gibi her model, hedeflenen uçağı tek bir sınıf olarak ele alırken, geri kalan yedi uçak diğer sınıfı kolektif olarak temsil etmiştir. Oluşturulan her dB değeri için 8'er farklı SVM modelleri ile ADS-B sinyalinin hedeflenen uçaktan gelip gelmediğini tahmin edebilmek için eğitilmiştir.




Şekil 5.4. Toplam 8 uçak için SVM sınıflandırmasında kullanılan örnek model

SVM sınıflandırmasının gerçekleştirilmesi için MATLAB araçları kullanıldı. Burada oluşturulan ICAO koduna göre etiketler ve RFF parmak izleri, SVM'de farklı kernel fonksiyonlarında sınıflandırmalara tabi tutulmuştur. Bu sınıflandırma modeli için konfigürasyon parametreleri Çizelge 5.1'de gösterilmiştir.

Çizelge 5.1. Tüm SVM sınıflandırmaları için kullanılan parametreler

| Parametre | Değer |
|---|---|
| Çekirdek Ölçek Parametresi (Kernel Scale Parameter) | Otomatik |
| Standartlaştırma (Standardize) | DOĞRU |
| Kutu Kısıtı (Box Constraint) | 1 |
| Polinom Çekirdek Fonksiyonu (Polynomial Kernel Function) | Otomatik |
| Optimizasyon Çözücü (Optimization Solver) | Tek Veri İteratif Algoritması (ISDA) |
| Önbellek Boyutu (Cache Size) | 1000 |
| ClipAlphas | DOĞRU |
| Nu (tek sınıflı öğrenme için v parametresi) (Nu ($v$ parameter for one-class learning)) | 0.5 |
| NumPrint | 1000 |
| Dış Değer Oranı, Ayrıntılı (OutlierFraction, Verbose) | 0 |
| Yinelemeleri Kaldır (RemoveDuplicates) | YANLIŞ |

Bu konfigürasyon parametrelerine göre her bir SNR değerinde (10dB, 15dB, 20dB, 25dB, 30dB) 8 farklı uçak için ayrı ayrı model oluşturulup ve 3 farklı kernel fonksiyonunda sınıflandırma tahminleri yapılmıştır.

Testlerin başarım oranı, MATLAB'da bulunan çapraz doğrulama (cross- validation) fonksiyonu ile elde edilmiştir. Çapraz doğrulama bir makine öğrenmesi modelinin genelleme yeteneğini değerlendirmek için kullanılan bir yöntemdir. Modelin, eğitim sırasında görmediği veriler üzerinde nasıl performans göstereceğine dair bir tahmin sunar. Burada en önemli değer kFold değeridir. Bu değer varsayılan olarak 10'dur. Veriyi rastgele 10 eşit parçaya bölüp 9'unu eğitim verisi 1'ini test verisi olarak sırayla kullanarak işlemi gerçekleştirir. $cvmodel = crossval(model)$ şeklinde kullanımı mevcuttur. Buradan elde edilen sonuca göre kfoldLoss ile tüm katmanlardaki hata değeri ortalaması sonucu yüzde olarak bulunur. Bu çalışmada, tüm uçakların her bir SNR değeri için çapraz doğrulama ile yüzdelik sonucu 10'ar kere bulunmuş ve bunun ortalaması alınmıştır. Bu sayede olabilecek tek seferlik hatalı sonuç elde edilmesinin önüne geçilerek daha tutarlı sonuçlar elde edilmiştir.

### 5.4. Sınıflandırma Sonuçları

Gerçekleştirilen polinom, doğrusal, dairesel tabanlı kernel fonksiyonlarının farklı SNR seviyelerine göre SVM testleri Çizelge 5.2, Çizelge 5.3 ve Çizelge 5.4'de gösterilmiştir. Bu sonuçlara göre; *polinom kernel fonksiyonunun* kullanıldığı SVM sınıflandırması Çizelge 5.2.'de gösterildiği gibi 10 dB, 15 dB, 20 dB, 25 dB ve 30 dB SNR değerleri için %92,07, %93,16, %93,53, %93,73 ve %93,91 ortalama doğruluğunu başarmıştır. *Doğrusal kernel fonksiyonunun* kullanıldığı SVM sınıflandırması Çizelge 5.3.'de gösterildiği gibi 10 dB, 15 dB, 20 dB, 25 dB ve 30 dB SNR değerleri için %91,27, %92,12, %92,18, %92,19 ve %93,33 ortalama doğruluğunu başarmıştır. Diğer yandan, dai*resel tabanlı kernel fonksiyonunun* kullanıldığı SVM sınıflandırması Çizelge 5.4.'de gösterildiği gibi 10 dB, 15 dB, 20 dB, 25 dB ve 30 dB SNR değerleri için %90,14, %90,64, %90,58, %90,63 ve %90,85 ortalama doğruluğunu başarmıştır.

Ortalama sınıflandırma doğruluğu sonuçları, polinom kernel fonksiyonlu SVM sınıflandırıcısının daha iyi sınıflandırma performansı sağladığını, buna karşın RBF kernel fonksiyonlu SVM sınıflandırıcısının her SNR seviyesinde bariz olarak daha düşük

sınıflandırma performansı sunduğunu göstermektedir. Bu tip SVM sınıflandırmalarında, etkinliği nedeniyle literatürde en popüler kernel fonksiyonu olarak bilinen RBF için beklenenden farklı bir sonuç ortaya çıkmıştır.

Ayrıca, elde edilen sonuçlarda RBF kernel fonksiyonunu kullanan SVM'nin, gürültüye karşı güçlü bir toleransı olduğunu ortaya koymaktadır. Çizelge 5.4.'de gösterildiği gibi 10 dB (minimum) ve 30 dB (maksimum) SNR seviyelerinde elde edilen ortalama doğruluklar ele alındığında, sınıflandırma performansında sadece %0,7'lik bir artış görülmüştür. Ancak, aynı SNR seviyelerindeki polinom ve doğrusal kernel fonksiyonlarına sahip SVM'ler incelendiğinde, sınıflandırma performansında %2'lik bir artış olduğu net bir şekilde görülebilir.

Özetle, SVM sınıflandırma testlerinden elde edilen minimum %90,14'lük doğruluk sonucuna göre, önerilen RFF yönteminin ADS-B sinyallerinin PSD benzersiz özelliklerini kullanarak sınıflandırılmasında başarılı olduğu görülmüştür. Bu durum, yöntemin çeşitli SNR seviyelerinde uygulanabilirliği açısından olumludur. Bunun yanında, doğrusal ve RBF kernel fonksiyonlarının yerine daha yüksek sınıflandırma doğruluğu elde edilmesine olanak sağlayan polinom kernel fonksiyonu, yapılacak sınıflandırma çalışmalarında daha başarılı sonuçlar sunacaktır.

Çizelge 5.2. Farklı SNR değerlerinde gerçekleştirilen polinom kernel fonksiyonlu SVM sınıflandırma (%) sonuçları

| SNR | Uçak 1 | Uçak 2 | Uçak 3 | Uçak 4 | Uçak 5 | Uçak 6 | Uçak 7 | Uçak 8 | Ortalaması |
|---|---|---|---|---|---|---|---|---|---|
| 10dB | 99,239 | 88,974 | 88,368 | 90,537 | 90,782 | 90,537 | 91,583 | 96,555 | 92,072 |
| 15dB | 99,466 | 90,138 | 89,713 | 91,241 | 92,282 | 91,684 | 93,359 | 97,385 | 93,158 |
| 20dB | 99,345 | 90,744 | 90,086 | 91,773 | 92,563 | 91,908 | 94,204 | 97,635 | 93,532 |
| 25dB | 99,313 | 90,908 | 90,460 | 92,256 | 92,601 | 92,267 | 94,273 | 97,799 | 93,735 |
| 30dB | 99,460 | 91,236 | 90,761 | 92,017 | 93,049 | 92,408 | 94,425 | 97,917 | 93,909 |

Çizelge 5.3. Farklı SNR değerlerinde gerçekleştirilen polinom kernel fonksiyonlu SVM sınıflandırma (%) sonuçları

| SNR | Uçak 1 | Uçak 2 | Uçak 3 | Uçak 4 | Uçak 5 | Uçak 6 | Uçak 7 | Uçak 8 | Ortalaması |
|---|---|---|---|---|---|---|---|---|---|
| 10dB | 99,284 | 87,966 | 87,603 | 89,497 | 89,681 | 90,009 | 90,733 | 95,414 | 91,273 |
| 15dB | 99,080 | 88,701 | 88,020 | 90,057 | 91,086 | 91,057 | 92,546 | 96,434 | 92,123 |
| 20dB | 98,655 | 88,830 | 88,259 | 90,055 | 91,244 | 91,356 | 92,693 | 96,391 | 92,185 |
| 25dB | 98,572 | 88,874 | 88,417 | 90,063 | 91,287 | 91,121 | 92,716 | 96,411 | 92,182 |
| 30dB | 98,704 | 88,928 | 88,724 | 90,259 | 91,457 | 91,443 | 92,727 | 96,379 | 93,328 |

Çizelge 5.4. Farklı SNR değerlerinde gerçekleştirilen RBF kernel fonksiyonlu SVM sınıflandırma (%) sonuçları

| SNR | Uçak 1 | Uçak 2 | Uçak 3 | Uçak 4 | Uçak 5 | Uçak 6 | Uçak 7 | Uçak 8 | Ortalaması |
|---|---|---|---|---|---|---|---|---|---|
| 10dB | 97,414 | 87,612 | 87,500 | 89,132 | 87,977 | 88,655 | 89,198 | 93,629 | 90,140 |
| 15dB | 97,810 | 87,787 | 87,526 | 89,500 | 88,629 | 89,296 | 90,092 | 94,474 | 90,639 |
| 20dB | 97,546 | 87,842 | 87,575 | 89,704 | 88,655 | 89,290 | 89,856 | 94,158 | 90,578 |
| 25dB | 97,307 | 88,032 | 87,621 | 89,894 | 88,790 | 89,480 | 89,761 | 94,138 | 90,628 |
| 30dB | 97,428 | 88,382 | 87,601 | 90,112 | 89,190 | 89,825 | 90,017 | 94,282 | 90,855 |

# 6. TARTIŞMA VE SONUÇ

## 6.1. Tartışma

Genel olarak, RFF yüksek güvenlik sağlayabilmesine karşın oldukça maliyetli bir çözümdür (Manesh ve Kaabouch, 2017). Uygulama maliyeti, tüm hava araçlarının sahip olduğu yayın kaynağından veri toplanmasını gerektirdiği için uygulanması zordur. Bu yayın kaynaklarına ait sinyallerin işlenip gerekli hesaplamaların yapılması yüksek kaynak gerektireceğinden pratikte bu işlemlerin yapılması önünde olumsuzluk teşkil eder. Bu bağlamda, bu çalışma ADS-B sinyallerinden oluşan küçük bir veri setini kullanarak uçak tanımlama için gerçek zamanlı uygulanabilir bir RFF yöntemi önermeyi amaçlamaktadır. Farklı SNR seviyelerinde önerilen yöntemin etkinliğini değerlendirmek üzere yapılan deneylerden elde edilen sonuçlar, polinom kernel fonksiyonuna sahip SVM'ye dayalı önerilen yöntemin, küçük bir veri setiyle bile uçakları sınıflandırmada iyi çalışabildiğini doğrulamaktadır.

Önerilen yöntemin etkinliğini değerlendirebilme amacıyla, farklı SNR düzeylerinde SDR'lar tarafından toplanan ADS-B sinyallerini kullanan mevcut RFF yöntemleriyle karşılaştırılabilir. Çizelge 3.1.'de verilen bilgileri özetlemek gerekirse, Louwen (2022) çalışmasındaki önerilen modelde kullanılan 10 dB SNR'a sahip sinyaller ile %44'lük bir doğruluk oranına ulaşılabilmiştir. Oldukça açıktır ki, %90'dan fazla sınıflandırma doğruluğu ile bu çalışmada önerilen yöntem, küçük veri seti boyutuna rağmen aynı SNR seviyesinde çok daha iyi performans sağlamaktadır. Agadakos vd. (2020) sunduğu çalışmada, 2 dB ile 5 dB arasında değişen SNR'lara sahip sinyaller kullanarak neredeyse %100 doğruluk oranına ulaşarak bu çalışmadan daha yüksek doğruluk sunmaktadır. Bunun yanında Jian vd. (2020), ADS-B sinyallerinin I/Q örneklerini, düşük SNR (1,9 - 13.3 dB) ile eğitip orta seviye SNR (5 - 2 dB) ile test ettiğinde en yüksek doğruluk oranı olan %92,5 oranını yakalayabilmiştir. Ancak, elde etmiş olduğu sonuçlar bu tez çalışmasında kullanılan I/Q örneklerinin sahip olduğu SNR değerlerinden oldukça farklı olduğu için herhangi bir kıyas yapmak uygun değildir. Ayrıca, Agadakos (2020) ve Jian vd. (2020), çalışmalarında önerilen yöntemler DL modellerine dayanmaktadır. Bu çalışmada oluşturulan veri setinin boyutundan oldukça fazladır. Nicolussi vd. (2020), Leonardi ve Gerardi (2020) ve Ying vd. (2019) çalışmalarında SNR değeri hakkında bilgi sunmadığı için bu tez çalışmasıyla kıyaslanması uygun değildir. Zha vd. (2020) yürüttüğü

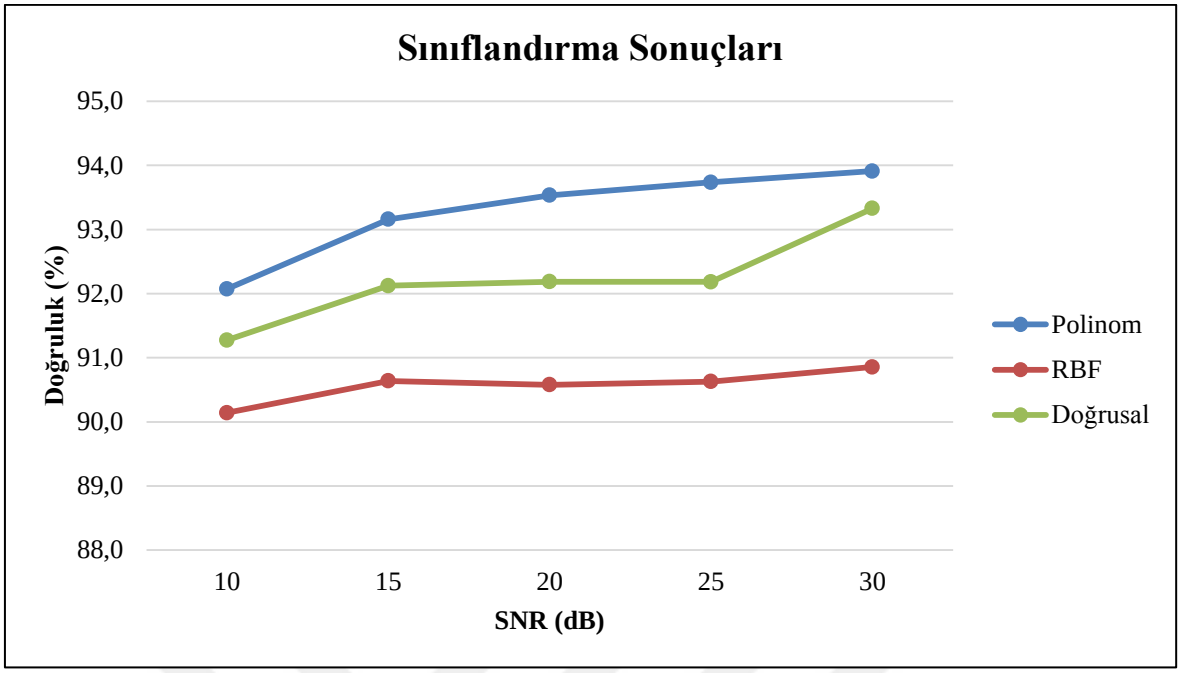
çalışmasında görüntüler ile eğitim ve test verileri oluşturup DL ile yüksek doğrulukta sonuçlar elde etmelerine karşın yöntemin farklılığı ve veri sayısının DL'e uygun olacak şekilde çok fazla olması bu çalışma ile tam kıyasa uygun değildir.

Bununla birlikte, bu tez çalışmasında önerilen yöntem 10 dB SNR'da küçük bir veri setiyle dahi umut vadedici sonuçlar elde etmektedir. Bu nedenle, önerilen modelin düşük hesaplama kaynaklarıyla gerçek dünya uygulamalarında etkin bir şekilde çalışabileceği düşünülmektedir.

Diğer yandan, bu akademik çalışmada hala net olmayan durumlar mevcuttur. Buna en temel örnek 10 dB SNR seviyesinin altında elde edilecek sonuca dair herhangi bir veri sunmamaktadır. 10 dB SNR'ın altında SNR değerine sahip sinyaller ile yapılacak testler önem arz etmektedir. Bu tarz düşük SNR seviyelerindeki sinyaller için daha fazla veriye ihtiyaç duyan DL modelleri daha uygun bir çözüm sunabilir (Krichen, 2023). Ancak, gerçek dünya ortamlarında uygulanabilir bir RFF yöntemi sağlamak için, CNN tabanlı modelin (bir sınıflandırıcı olarak) küçük bir veri seti boyutuyla bile basit ve etkili olması gerekmektedir.

### 6.2. Sonuç

Bu çalışmada, RFF tabanlı bir uçaklarda bulunan yayın kaynaklarının sınıflandırmasına yönelik bir yöntem önerilmektedir. Önerilen yöntem, RFF uygulaması için ayırt edici bir özellik olarak ADS-B sinyallerinin PSD'sini kullanmaktadır. Farklı SNR seviyelerinde (10 – 30 dB) uçakları tanımlamak için üç farklı kernel fonksiyonuna sahip (polinom, doğrusal ve RBF kernel) SVM kullanılmaktadır. Elde edilen deneysel sonuçlara göre, polinom kernel SVM sınıflandırıcısıyla daha yüksek sınıflandırma performansı elde edilmiştir. Daha net belirtmek gerekirse, polinom kernel fonksiyonlu SVM sınıflandırıcısının genel sınıflandırma doğruluğunun 10 dB'de %92.07, 15 dB'de %93.16, 20 dB'de %93.53, 25 dB'de %93.73 ve 30 dB'de %93.91 olduğu bulunmuştur.




Şekil 6.1. SVM sınıflandırmasının kernel fonksiyonlarına göre sonuçları

Deneylerden elde edilen sonuçlar ayrıca, RBF kernel fonksiyonuna sahip SVM'nin güçlü bir gürültü toleransına sahip olduğunu göstermektedir. 10 dB ve 30 dB SNR seviyelerinde, polinom ve doğrusal kernel fonksiyonlu SVM'ye kıyasla sınıflandırma performansında sadece %0.7'lik bir artış mevcuttur. Diğer kernel fonksiyonlarına göre daha az doğruluğa sahip olsa da deneylerden elde edilen %90.14'lük bir sınıflandırma doğruluğu, RFF uygulamasında uçakları sınıflandırmak için ADS-B sinyallerinin PSD'sinin özellik olarak kullanılabileceğini doğrulamaktadır. Ayrıca, düşük maliyetli ve yaygın olarak bulunan bir SDR tarafından toplanan ADS-B sinyalleri içeren küçük bir veri setiyle bile RFF tabanlı uçak tanımlamanın mümkün olduğu gösterilmiştir.

Gelecekteki çalışmalarımızda, DL yaklaşımlarına dayalı bir RFF yöntemi önermeyi amaçlıyoruz. Amacımız, daha düşük SNR'da (≤10 dB) uçakların tanımlanması için basit bir CNN tabanlı sınıflandırıcı geliştirmektir. Ancak, veri setinin boyutunun RFF'in performansında belirleyici bir faktör olması beklenmektedir. Bu nedenle, veri setini artırmak gerekebilir. Gelecekte, bu tür bir yöntemin geliştirilmesi ve performansı üzerine kapsamlı bir çalışma sunulacaktır.

# KAYNAKLAR


Agadakos, I., Agadakos, N., Polakis, J. ve Amer, M. R. (2020). *Chameleons' oblivion: Complex-valued deep neural networks for protocol-agnostic RF device fingerprinting.* 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Genoa, Italy, 322-338.

Ali, A. M., Uzundurukan, E. ve Kara, A. (2019). Assessment of features and classifiers for Bluetooth RF fingerprinting. *IEEE Access*, 7, 50524-50535.

Amin, S., Clark, T., Offutt, R. ve Serenko, K. (2014). *Design of a cyber security framework for ADS-B based surveillance systems.* 2014 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 304-309.

An-na, W., Yue, Z., Yun-tao, H. ve Yun-lu, L. I. (2010). *A novel construction of SVM compound kernel function.* 2010 International Conference on Logistics Systems and Intelligent Management (ICLSIM), Harbin, China, 1462-1465.

Alghamdi, F., Alshrahani, A. ve Hamza, N. (2018). Effective security techniques for automatic dependent surveillance-broadcast (ADS-B). *International Journal of Computer Applications*, 180(26), 23-28.

Bostancı, M. O. (2021). *Otomatik bağımlı izleme sistemi (ADS-B) alıcı yer istasyonu tasarımı*. Yüksek Lisans Tezi, Eskişehir Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü, Eskişehir.

Bottou, L. ve Lin, C. J. (2007). Support vector machine solvers. *Large scale kernel machines*, 3(1), 301-320.

Cook, E. (2015). *ADS-B, friend or foe: ADS-B message authentication for NextGen aircraft*. 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, New York, NY, USA, 1256-1261.

Giannessi, F. (2007). On the theory of Lagrangian duality. *Optimization Letters*, 1(1), 9-20.

Hableel, E., Baek, J., Byon, Y. J. ve Wong, D. S. (2015). *How to protect ADS-B: Confidentiality framework for future air traffic communication.* 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Hong Kong, China, 155-160.

Jian, T., Rendon, B. C., Ojuba, E., Soltani, N., Wang, Z., Sankhe, K., Gritsenko, A., Dy, J., Chowdhury, K. ve Ioannidis, S. (2020). Deep learning for RF fingerprinting: A massive experimental study. *IEEE Internet of Things Magazine*, 3(1), 50-57.

Kim, Y., Jo, J. Y. ve Lee, S. (2017). ADS-B vulnerabilities and a security solution with a timestamp. *IEEE Aerospace and Electronic Systems Magazine*, 32(11), 52-61.

Krichen, M. (2023). Convolutional neural networks: A survey. *Computers*, 12(8), 151.

Kovell, B., Mellish, B., Newman, T. ve Kajopaiye, O. (2012). *Comparative analysis of ADS-B verification techniques.* The University of Colorado, Boulder, 4.

Leonardi, M., Piracci, E. ve Galati, G. (2014). *ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions.* 2014 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), Rome, Italy, 41-46.

Leonardi, M. ve Gerardi, F. (2020). Aircraft mode S transponder fingerprinting for intrusion detection. *Aerospace*, 7(3), 30.

Leonardi, M. ve Sirbu, G. (2021). Ads-b crowd-sensor network and two-step kalman filter for gnss and ads-b cyber-attack detection. *Sensors*, 21(15), 4992.

Louwen, A. (2022). *Radio Frequency Fingerprinting for Aircraft Identification*, Master Thesis, Delft University of Technology Aerospace Engineering, Delft.

Manesh, M. R. ve Kaabouch, N. (2017). Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *International Journal of Critical Infrastructure Protection*, 19, 16-31.

McCallie, D., Butts, J. ve Mills, R. (2011). Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*, 4(2), 78-87.

Mirzaei, K. F., De Carvalho, B. P. ve Pschorn, P. (2019). *Security of ADS-B: Attack scenarios.* EasyChair, Tech. Rep.

Nicolussi, A., Tanner, S. ve Wattenhofer, R. (2021). *Aircraft fingerprinting using deep learning.* 2020 28th European Signal Processing Conference (EUSIPCO), Amsterdam, Netherlands, 740-744.

Nolan, M. S. (2011). *Fundamentals of Air Traffic Control, 5th Edition.* Delmar Cengage Learning, 36-41.

Pöpper, C., Strasser, M. ve Capkun, S. (2009). *Jamming-resistant broadcast communication without shared keys.* USENIX security Symposium, Zürich, Switzerland, 231-248.

Reisman, R. J. (2019). *Air traffic management blockchain infrastructure for security, authentication, and privacy.* AIAA Scitech Forum (No. ARC-E-DAA-TN63825), San Diego, CA, USA.

Ren, P., Wang, J., Song, H., Zhang, P. ve Ban, T. (2019). A novel multi-criteria preamble detection algorithm for ADS-B signals. *IEEE Access*, 7, 97319-97332.

Sarraf, S. (2017). EEG-based movement imagery classification using machine learning techniques and Welch's power spectral density estimation. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, 33(1), 124-145.

Schafer, M., Lenders, V. ve Martinovic, I. (2013). *Experimental analysis of attacks on next generation air traffic communication.* Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28, 2013. Proceedings 11, 253-271. Springer Berlin Heidelberg.

Singh, D. ve Singh, B. (2020). Investigating the impact of data normalization on classification performance. *Applied Soft Computing*, 97, 105524.

Slimane, H. O., Benouadah, S., Al Shamaileh, K., Devabhaktuni, V. ve Kaabouch, N. (2022). *ADS-B message injection attack on UAVs: assessment of SVM-based detection techniques.* 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 405-410.

Smith, S. (2003). *Digital signal processing: a practical guide for engineers and scientists*. Newnes, 277-284.

Soyertem, H. (2022). *Hava Trafik Kontrol Gözetim Sistemleri ve Hizmetleri*. Devlet Hava Meydanları İşletmesi Genel Müdürlüğü, 52-53.

Strasser, M., Popper, C., Capkun, S. ve Cagalj, M. (2008). *Jamming-resistant key establishment using uncoordinated frequency hopping.* 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 64-78.

Strohmeier, M., Lenders, V. ve Martinovic, I. (2013). *Security of ADS− B: State of the Art and Beyond.* DCS, Report, University of Oxford.

Sun, J. (2021). *The 1090 megahertz riddle: a guide to decoding mode s and ads-b signals*. TU Delft OPEN Publishing.

Sun, J., Olive, X., Strohmeier, M., Schafer, M., Martinovic, I. ve Lenders, V. (2021). *OpenSky report 2021: Insights on ads-b mandate and fleet deployment in times of crisis.* 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC), San Antonio, TX, USA, 1-10.

Suski II, W. C., Temple, M. A., Mendenhall, M. J. ve Mills, R. F. (2008). *Using spectral fingerprints to improve wireless network security.* IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, New Orleans, LO, 1-5.

Toonstra, J. ve Kinsner, W. (1995). *Transient analysis and genetic algorithms for classification.* IEEE WESCANEX 95. Communications, Power, and Computing. Conference Proceedings, Winnipeg, MB, Canada, 2, 432-437.

Toonstra, J. ve Kinsner, W. (1996). *A radio transmitter fingerprinting system ODO-1*. Proceedings of 1996 Canadian Conference on Electrical and Computer Engineering, Calgary, AB, Canada, 1, 60-63.

U.S. Department of Transportation (2018). *Surveillance and Broadcast Services Description Document, 04.*

Wu, Z., Shang, T. ve Guo, A. (2020). Security issues in automatic dependent surveillance-broadcast (ADS-B): A survey. *IEEE Access*, 8, 122147-122167.

Yang, H., Zhou, Q., Yao, M., Lu, R., Li, H. ve Zhang, X. (2018). A practical and compatible cryptographic solution to ADS-B security. *IEEE Internet of Things Journal*, 6(2), 3322-3334.

Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L. ve Poovendran, R. (2019). *Detecting ADS-B spoofing attacks using deep neural networks.* 2019 IEEE conference on communications and network security (CNS), Washington, DC, USA, 187-195.

Zha, H., Tian, Q. ve Lin, Y. (2020). *Real-world ADS-B signal recognition based on radio frequency fingerprinting.* 2020 IEEE 28th international conference on network protocols (ICNP), Madrid, Spain, 1-6.



*Gazili olmak ayrıcalıktır*