T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

İNSANSIZ HAVA ARAÇLARINDA YENİLİK TABANLI İZİNSİZ GİRİŞ TESPİTİ

Onur AYVA

Yüksek Lisans Tezi

SAVUNMA TEKNOLOJİLERİ ANABİLİM DALI

TEMMUZ 2023

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Savunma Teknolojileri Anabilim Dalı

Yüksek Lisans Tezi

İNSANSIZ HAVA ARAÇLARINDA YENİLİK TABANLI İZİNSİZ GİRİŞ TESPİTİ

Tez Yazarı
Onur AYVA

Danışman
Prof. Dr. Sami EKİCİ

TEMMUZ 2023
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Savunma Teknolojileri Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	İnsansız Hava Araçlarında Yenilik Tabanlı İzinsiz Giriş Tespiti
Yazarı:	Onur AYVA
İlk Teslim Tarihi:	12.06.2023
Savunma Tarihi:	12.07.2023

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

		İmza
Danışman:	Prof. Dr. Sami EKİCİ Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Prof. Dr. Resul ÇÖTELİ Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Mehmet ÜSTÜNDAĞ Turgut Özal Üniversitesi, Mühendislik Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Burhan ERGEN
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "İnsansız Hava Araçlarında Yenilik Tabanlı İzinsiz Giriş Tespiti" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

12.07.2023

Onur AYVA

ÖNSÖZ

Bu tez çalışması Fırat Üniversitesi Fen Bilimleri Enstitüsü Savunma Teknolojisi Yüksek Lisans programında hazırlanmıştır. İnsansız hava araçlarında yenilik tabanlı izinsiz giriş tespiti konusunda literatüre bakıldığında sınırlı sayıda çalışmaya rastlanılmaktadır. Yapılan testlerin ve çalışmaların çoğunun ise benzetim verileri ile gerçekleştirildiği ve daha çok klasik çok sınıflı sınıflandırıcılar kullanılarak yapıldığı görülmektedir. Bu çalışmada, insansız hava araçlarına düzenlenen izinsiz girişlere yönelik öğrenilmiş ve imza tabanlı bir yaklaşım yerine yenilik tabanlı, tek sınıflı bir sınıflandırma ve tespit sistemi önerilmektedir.

Tez süreci boyunca tecrübeleriyle bana yol gösteren, ufkumu açan ve benden desteklerini esirgemeyen danışman hocam Prof. Dr. Sami EKİCİ'ye sonsuz teşekkürlerimi ve minnettarlığımı sunarım.

Verdikleri destek ve ileriye donuk fikirler için Dr. Arş. Gör Fatih ÜNAL'a teşekkür ederim. Ayrıca bütün zorluklara rağmen beni sürekli destekleyen aileme teşekkürlerimi sunarım.

Onur AYVA
ELAZIĞ, 2023

İÇİNDEKİLER

Sayfa

ÖZET

İnsansız Hava Araçlarında Yenilik Tabanlı İzinsiz Giriş Tespiti

Onur AYVA

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Savunma Teknolojileri Anabilim Dalı

Temmuz 2023, Sayfa: xiii + 83

Bu çalışma, yenilik tabanlı izinsiz girişler neticesinde oluşacak arızaların veya anormalliklerin tespiti için farklı makine öğrenmesi yöntemlerinin performansını değerlendirmeyi amaçlamaktadır. Motor, kanatçık, dümen ve asansör arızaları üzerinde odaklanılarak, tek sınıflı-destek vektör makineleri (OC-SVM), tek sınıflı-rastgele orman algoritması (OC-RF), yerel aykırılık faktörü algoritması (LOF) ve otomatik kodlayıcı (Autoencoder) yöntemleri kullanılmış ve sonuçlar doğruluk, hassasiyet, duyarlılık ve F-skor metrikleriyle değerlendirilmiştir.

OC-SVM yöntemi motor, kanatçık, dümen ve asansör arızaları için oldukça başarılı bir performans ortaya koymuştur. Bu yöntemde, tüm performans metrikleri 1 değerini alarak arızaları tespit etme konusunda yüksek bir doğruluk ve etkinlik sağlamıştır.

Benzer şekilde, OC-RF yöntemi de motor, kanatçık, dümen ve asansör arızalarının tespitinde yüksek bir performans sergilemiştir. Tüm metriklerin 1 değerine sahip olması, bu yöntemin de arıza tespiti için güvenilir bir seçenek olduğunu göstermektedir.

LOF yöntemi, diğer yöntemlere kıyasla biraz daha düşük bir performans sergilese de yine de başarılı sonuçlar vermiştir. Motor, kanatçık, dümen ve asansör arızaları için doğruluk, hassasiyet, duyarlılık ve F-skor metrikleri diğer yöntemlere göre biraz daha düşük değerlere sahiptir. Bu değerler 0,998 olarak elde edilmiştir.

Otomatik kodlayıcı yöntemi ise tüm arıza türleri için OC-SVM ve OC-RF yöntemleriyle benzer sonuçlar elde etmiştir. Doğruluk, hassasiyet, duyarlılık ve F-skor metrikleri 1 olarak hesaplanmış ve böylece bu yöntemin arıza tespitindeki başarısı ve güvenilirliği kanıtlanmıştır.

Sonuç olarak, yapılan bu çalışma motor, kanatçık, dümen ve asansör arızalarının tespiti için farklı makine öğrenimi yöntemlerinin etkisini değerlendirmiştir. OC-SVM, OC-RF ve Autoencoder yöntemleri tam performans sergilerken, LOF yöntemi diğer yöntemlerden biraz daha düşük bir performansa sahip olmuştur. Bu sonuçlar, arıza tespiti için farklı yöntemlerin değerlendirilmesi ve seçiminde rehberlik sağlamaktadır.

Gelecekteki çalışmalar, daha geniş veri kümeleri ve yeni özelliklerin eklenmesi gibi faktörlerin etkisini değerlendirebilir ve arıza tespit sistemlerinin daha da geliştirilmesine katkıda bulunabilir. Tez çalışması, arıza tespiti alanında çalışan araştırmacılar ve endüstri uzmanları için faydalı bir kaynak olabilir ve daha ileri çalışmalara ilham verebilir.

Anahtar Kelimeler: İnsansız hava araçları, Yenilik tabanlı izinsiz giriş tespiti, Makine öğrenmesi, Tek sınıflı sınıflandırıcı.

ABSTRACT

Novelty Based Intrusion Detection in Unmanned Aerial Vehicles

Onur AYVA

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Defence Technologies

July 2023, Pages: xiii + 83

This study aims to evaluate the performance of different machine learning methods for the detection of faults or anomalies due to novelty-based intrusions. Focusing on engine, aileron, rudder, and elevator faults, single-class-support vector machines (OC-SVM), single-class-random forest algorithm (OC-RF), local outlier factor algorithm (LOF) and autoencoder (Autoencoder) methods are used and the results are evaluated with accuracy, precision, sensitivity and F-score metrics.

The OC-SVM method performed very well for engine, aileron, rudder and elevator faults. In this method, all performance metrics took the value of 1, providing high accuracy and efficiency in detecting faults.

Similarly, the OC-RF method also showed a high performance in detecting engine, aileron, rudder and elevator failures. The fact that all metrics have a value of 1 indicates that this method is also a reliable option for fault detection.

Although the LOF method showed a slightly lower performance compared to the other methods, it still gave successful results. The accuracy, sensitivity, precision, sensitivity and F-score metrics for engine, aileron, rudder and elevator faults have slightly lower values than the other methods. These values were obtained as 0.998.

Autoencoder method obtained similar results with OC-SVM and OC-RF methods for all failure types. Accuracy, precision, sensitivity and F-score metrics were calculated as 1, thus proving the success and reliability of this method in fault detection.

In conclusion, this study evaluated the effect of different machine learning methods for engine, aileron, rudder and elevator fault detection. The OC-SVM, OC-RF and Autoencoder methods performed well, while the LOF method had a slightly lower performance than the other methods. These results provide guidance in the evaluation and selection of different methods for fault detection.

Future work can evaluate the impact of factors such as larger datasets and the addition of new features and contribute to the further development of fault detection systems. The thesis work can be a useful resource for researchers and industry experts working in the field of fault detection and can inspire further work.

Keywords: Unmanned aerial vehicles, Novelty-based intrusion detection, Machine learning, One-class classifier.

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Simgeler

gr	: Gram
kg	: Kilogram
m	: Metre
cm	: Santimetre
mm	: Milimetre
3G	: 3. Nesil
4G	: 4. Nesil
5G	: 5. Nesil
φ	: Çekirdek İşlevi
ϵ_i	: Değişken Değer
p	: Karar Değeri
v	: Uzak Noktaların Oranı
$h(x)$	: Karar Fonksiyonu
γ_e	: Heterojen Entropi İndeksi
γ_G	: Gini İndeksi
p_l	: Nesnelerin Oranı
B	: Öyküleme Kopyalarının Sayısı
$t^i x^i$	: Örnek i Üzerine İnşa Edilen Ağaç
W,B	: Kod Çözücünün Ağırlık ve Yanlılık Matrisi
f, g	: Kod Çözücünün Ağırlık ve Yanlılık Fonksiyonu

Kısaltmalar

MALE	: Orta İrtifa Uzun Menzilli
İHA	: İnsansız Hava Aracı
ABD	: Amerikan Birleşik Devletleri
AB	: Avrupa Birliği
IRNSS	: Hindistan Bölgesi Navigasyon Uydu Sistemi
YT	: Yenilik Tespiti
İGTS	: İzinsiz Giriş Tespit Sistemi
GPS	: Küresel Konumlama Sistemi
RESCHU	: Heterojen İnsansız Hava Araçların Denetleyici Kontrolü için Araştırma Ortamı
OC-SVM	: Tek Sınıflı Destek vektör Makinesi
SVM	: Destek Vektör Makinası
LOF	: Yerel Aykırı Destek Faktörü
IGTS	: Saldırı Tespit Sistemi
STS	: Saldırı Tespit Sistemi
IMU	: Atalet Ölçüm Birimi (Yeni Nesil Navigasyon Sensörü (Hız, Konum, Eğim, İvme))
Lrd	: Yerel Erişebilirlik Yoğunluğu
HALE	: Yüksek İrtifa Uzun Menzilli
VTOL	: Sabit Kanatlı Hibrit İHA
TAİ	: Türk Havacılık ve Uzay Sanayi
LTE	: Uzun Süreli Gelişim (Lang Term Evolution (4.5G))
FPV	: Birinci Kişi Görünümü

RF	: Radyo Frekansı
GNSS	: Küresel Uydu Seyrüsefer Sistemleri
HPM	: Yüksek Güçlü Mikrodalga
DoS	: Hizmet Reddi Saldırıları
GVZF	: Gözlemlenebilen Varış Zaman Farkı
EUROUVS	: Avrupa İnsansız Hava Sistemi Kurumu
ESC	: Elektronik Devre Kontrolü
OC-RF	: Tek Sınıflı Rasgele Orman Sınıflandırıcısı
RF	: Rasgele Orman Sınıflandırıcısı
Nu	: Eğim Verisindeki Anormallik
RESCHU	: Heterojen İnsansız Araçların Denetleyici Kontrolü için Araştırma Ortamı
IPS	: İzinsiz Giriş Önleme Sistemi
ReLU	: Doğrultulmuş Lineer Birim (Rectified Linear Unit)

1. GİRİŞ

Günümüzde insansız hava araçlarına (İHA) olan ilginin artması, bu alanlarda oluşabilecek güvenlik tehditlerini de beraberinde getirmektedir. Türk hava kurumuna göre; İHA'lar, içinde pilot ve yolcusu olmayan, sadece amaca uygun ekipman (video, kamera, fotoğraf makinesi, GNSS, lazer tarama cihazı, vb.) taşıyan, uzaktan kumandalı veya otomatik olarak görevini icra edebilen bir çeşit uçaktır [1]. İHA, ilk olarak 1846 yılında Avustralya tarafından Venedik şehrine, pilotsuz balonlarla yapılan hava saldırıları ile kullanılmaya başlamıştır. Bu tarihten sonra, ilk insansız uçak 1916 yılında tasarlanmış ve ilk uçuşunu 1918 yılında gerçekleştirmiştir. İHA'ların kullanımı 2. Dünya Savaşı Bosna-Hersek, Kosova, Afganistan, Irak ve Suriye gibi çatışma alanlarında gelişerek devam etmiştir [2]. İHA'lar; askeri, afet, kurtarma, yangın söndürme, ilaç temini, trafik izleme, sinema, hobi ve tarım gibi birçok alanda kullanılmaktadır. Ucuz hava gözetimi ve araştırmaları için geniş çapta faydaları olduğu kabul görmektedir. İHA'ların kullanım alanlarının artmasından dolayı yeni güvenlik tehditleri ortaya çıkmaktadır. Bunun sebebi, bilinçli veya bilinçsiz bir şekilde saldırı amaçlı da kullanılmasıdır. Polis operasyonları, askeri operasyonlar, düşman gözetimi, düşman takibi, terör sığınakların bulunması gibi hassas ve kritik uygulamalar için kullanılmaktadır. Bu profesyonel İHA'ların bile çeşitli güvenlik açıklarına sahip olduğu görülmektedir.

İHA'ların, günümüzde askeri birçok alanda üstün başarıları olduğu görülmektedir. İstihbarat faaliyetleri günümüzde değişkenlik göstermekte olan İHA'lar, anlık olarak istihbarat sağlama kabiliyetini icra etmekte ve operasyonel görevlileri de üstlenmektedir. Bu görevle birlikte yeni nesil askeri havacılık anlayışında, temel değişikliklerden en önemlisi, pilot olmadan onun yerine yapay zekâ kullanılarak profesyonel bir şekilde kullanılabilmektedir.

Havacılık endüstrisi, ülkelerin teknolojide elde ettikleri başarıları gelişmişlik seviyelerinin bir aynası olarak görmektedir. İHA, pilotun yerden kontrol etmesiyle faaliyetlerini gerçekleştirmesinin yanı sıra ulaşılması güç olan noktalara, operasyon faaliyetlerini yapay zekânın, bir pilotun anlık duygularıyla karar verip hareketi geçebileceği, seviyeye gelmesi öngörülmektedir. Bu durum için BAYKAR'ın geliştirmiş olduğu Kızıl Elma en büyük örneklerden biridir. Böylelikle İHA'lar politik, ekonomik ve de siyasi bir güç unsuru haline gelmiştir.

İHA'lar gün geçtikçe gelişim göstermesi, boyut küçülmesi veya büyümesi, maliyet azalması gibi birçok fonksiyonlu ve kabiliyetli hale gelmektedir. Devletlerin kullanımlarının yanı sıra özel sektöründe ciddi manada yatırım yaptığı görülmektedir. İnsansız hava araçları askeri ve ticari alanlarda gelişimlerinden kaynaklı kötü niyetli kişilerin elinde tehdit unsuru oluşturmaktadır. İHA'lara yapılan saldırıların genel manada uzaktan haberleşme metoduyla yapıldığı görülmektedir. Hava araçlarında kontrol, veri iletişimi ve veri iletiminde kullanılan radyo frekansı, Wi-fi, Bluetooth, 3G, 4G, 5G, LTE ve GPS gibi çeşitli kablosuz haberleşme teknolojilerinde kullanılmaktadır. Küresel konumlama sistemleri İHA'lar için hassas konum bilgisi sağlamasından

dolayı büyük bir önem taşımaktadır. Bunun gibi kullanılan iletişim yöntemleri, İHA'lara yönelik saldırıları arttırmaktadır. Bu tür sistemlere yönelik saldırılar için koruyucu önlemlere ihtiyaç duyulmaktadır.

GPS ilk olarak askeri sistemlerde kullanılırken ilerleyen zamanlarda sivil kullanımlara da açılmıştır. Gerek endüstri gerekse günlük hayatta konum, hız ve zaman gibi kavramlara ihtiyaç duyulmuştur. GPS sistemi yönetiminin Amerika Birleşik Devleti'nde (ABD) olması ve özellikle sivil alanda yapısı gereği saldırılara karşı korunmasız olması sebebiyle farklı ülkeler tarafından çeşitli küresel konumlama sistemleri geliştirilmiştir. Rusya tarafından GLONASS, Avrupa Birliği (AB) tarafından Galileo, Çin tarafından BeiDou ve Hindistan tarafından IRNSS konumlama sistemleri geliştirilmiştir. Ancak GPS dışındaki sistemler henüz yeterlilik seviyesine ulaşmadığı için dünyada genel olarak her alanda GPS kullanılmaktadır [3].

GPS sistemi güvenlik zafiyetleri yönünden, özellikle yapısının açık, şifresiz olması ve herhangi bir kimlik doğrulama mekanizmasına sahip olmamasından dolayı, hava araçlarına yapılan saldırıların bu yönde yapılması muhtemeldir. Bu zayıflığın neticesinde GPS sistemi üzerinde akademik alanda çalışmalar yapılmaya başlanmıştır. Bu çalışmalar genellikle GPS sinyallerinin kesilmesi, engellenmesi, radyo frekansı parazitleri oluşturulması veya oynanması ve gönderilen frekansın neredeyse birebir benzetilmesi ile aldatma (spoofing) saldırı gibi yöntemler kullanılmaktadır. Bu saldırıların gerçekleşmesi durumunda İHA'larda uçuş sırasında hareket ve manevralarında değişiklikler meydana gelmektedir. Bu değişiklikler sensör verileri ile okunmakta ve hava aracının hareketlerinde görülmektedir. Saldırılar neticesinde oluşan bu anormal durumların tespit edilip önlem alınması gerekmektedir.

İnsansız hava araçları endüstriyel koordinat sistemleri gözetimi, kolluk kuvvetleri ve askeri operasyonlar dâhil olmak üzere çok sayıda endüstride faydalı bir teknoloji olduğu kanıtlanmıştır. İHA'lar kablosuz protokolleri ve terörle mücadele çalışma ortamlarına olan yoğun bağımlılıkları nedeniyle büyük bir tehdit ortamıyla karşı karşıya kalmaktadır. Ülkemiz Drone ve İHA'lar alanında dünyada ilk 4 ülke arasında yer almaktadır. İHA'lara yönelik saldırıların olması kaçınılmaz bir durum oluşturmaktadır. Bu risklere karşı bir savunma sistemi geliştirmenin ilk adımı ise bu saldırıların ve saldırı tipinin tespit edilmesidir. Bu çalışmanın temel amacı İHA'lara yönelik olarak sisteme enjekte edilen bozucu sinyallerin neticesinde oluşacak anormalliklerin ve arızaların mümkün olduğu kadar erken bir sürede tespit edilmesidir. Literatüre bakıldığında bu alanda yapılan bilimsel çalışma ve kaynakların sınırlı sayıda olduğu görülmektedir. İstenilen miktarda ve nitelikte etiketlenmiş halka açık veri seti bulunmaması ve bu alandaki deneysel çalışmaların maliyetli olması, yapılan çalışma ve araştırma sayısının az olmasında önemli bir etken olarak göze çarpmaktadır. İHA'lara yapılan siber saldırılara örnek olarak Suudi Arabistan'ın en büyük petrol rafinerisi Sudi Aramco'ya yapılan saldırıdır. Bu olay petrol üretiminin 5,7 milyon varil azalmasına neden olmuştur. İHA'lar yapılan saldırılar sonucunda bazen uzaktan kapatılabilir, kaçırılabilir,

uçup gidebilir veya çalınabilmektedir. İHA'ların ulusal hava sahası entegrasyonuna yönelik planlar devam ederken, bu entegrasyonun önündeki kritik noktalarından biri bu sistemlerin emniyetini ve güvenliğini sağlamaktır. Güvenlik endişeleri, iletişimlerin şifrelenmemiş olması ve İHA mimarisinin yaygın olarak bilindiği sivil uygulamalarda daha yoğun bir biçimde göze çarpmaktadır. İHA'lara yönelik güvenlik tehditlerinin doğasında, dinleme gibi pasif gizlilik ihlallerinden, karıştırma ve sahtekârlık gibi aktif bütünlük ihlallerine geçiş vardır. İHA'lara yapılan saldırılar, giderek daha akıllı hale gelmekte ve İHA'ları gizlice tehlikeye atmak için çok daha karmaşık mekanizmalar kullanılmaktadır. Böyle bir senaryoda, kötü niyetli siber fiziksel saldırıları aktif olarak tespit edebilen ve azaltabilen bir sistem geliştirmek esas olacaktır. Tespit edilemeyen saldırıların yukarıda bahsedildiği gibi maddi, manevi ve siyası birçok büyük kayıplara yol açtığı görülmektedir.

Bu tez çalışmasının temel amacı, özellikle son yıllarda birçok alanda kullanılan İHA'lara yönelik olarak yapılan siber saldırıların tespit edilmesidir. Bu temel amaca yönelik olarak insansız hava araçlarında izinsiz giriş tespiti için yenilik tabanlı tek sınıflı yapay zeka yöntemleri önerilmiştir. Mevcut uçuş günlüklerinden elde edilen etiketsiz İHA saldırı tespit veri kümelerinin tek sınıflı sınıflandırıcılar ile nasıl eğitileceğine yer verilecektir. Gerçek uçuş günlüklerinden elde edilen veri setlerini kullanarak çeşitli sınıflandırıcıların performansları değerlendirilecektir.

İnsansız hava araçlarına yapılan izinsiz girişler sonucunda oluşan anormal durumların tespitine yönelik hipotezler sıralandığında;

- Etiketlenmemiş veri seti bulmada yaşanan zorluklar, literatürde yapılan bazı çalışmaların sadece belirli saldırılara ve İHA platformlarına hitap etmesi, veri setinin işlenmesi ve kullanılacak algoritmanın seçimi gibi zorlukların üstesinden gelebilmek için bu çalışmada Yenilik Tespiti (YT) tabanlı bir akıllı İzsiniz Giriş Tespit Sistemi (İGTS) geliştirilecektir.
- YT sistemlerini diğer yöntemlerden ayıran en önemli üstünlüğü eğitim için etiketli veriye ihtiyaç duymamasıdır. Yenilik tabanlı İGTS bu özelliği ile rahatlıkla farklı İHA platformlarına da uygulanabilecektir.
- Sınıflandırıcı eğitiminde yararlanılacak veri seti sadece güvenilir uçuşlardan elde edilen uçuş günlüklerini içerecek, eğitilen tek sınıflı sınıflandırıcılar normal uçuş verilerinden farklı (yeni) bir veriyle karşılaştığında bunu anormal durum/izinsiz giriş olarak algılayacaktır.

Tez çalışmasının ikinci bölümünde literatürde yapılan ilgili çalışmalara değinilmiştir. Üçüncü bölümde İHA'ların sınıflandırılması, haberleşmesi ve müdahale yöntemlerine değinilmiştir. Dördüncü bölümde donanım, veri seti, kullanılan yöntem ve arızalar hakkında bilgi verilmiştir. Beşinci bölümde izinsiz giriş tespiti ve yöntemleri hakkında detaylı bilgi verilmektedir. Bu bilgilerin yanı sıra kullanılan OC-SVM, OC-RF, LOF ve Autoencoder sınıflandırıcıları hakkında bilgi verilmekte ve bu yöntemlerin benzetim sonuçlarına değinilmektedir. Altıncı ve son bölümde ise, tez çalışması sonuçlandırılmıştır.

2. LİTERATÜR ÇALIŞMASI

Günümüzde İHA'lar hızla yaygınlaşan bir teknoloji haline gelmiştir ve birçok alanda kullanılmaktadır. İHA'lar, hava fotoğrafçılığından insansız teslimat sistemlerine, tarım sektöründen güvenlik uygulamalarına kadar geniş bir yelpazede kullanım potansiyeline sahiptir. Ancak artan İHA trafiği, izinsiz girişler ve güvenlik tehditlerini de ortaya çıkarmaktadır. İnsansız hava araçlarına yönelik izinsiz girişler, özel alanların ihlal edilmesi, veri güvenliği riskleri ve hatta potansiyel saldırılar gibi sorunlara yol açabilmektedir.

Bu nedenle, insansız hava araçlarında izinsiz giriş tespiti, bu teknolojinin güvenli ve sorunsuz bir şekilde kullanılabilmesi için önemli bir konu haline gelmiştir. Literatürde yapılan çalışmalar, farklı yaklaşımlar ve yöntemler kullanarak izinsiz girişlerin tespit edilmesi ve engellenmesi üzerine odaklanmaktadır. Bu çalışmalarda, yapay zekâ ve makine öğrenimi gibi alanlardan faydalanılarak etkili çözümler geliştirilmeye çalışılmaktadır.

İHA'ların saldırıya uğraması sonucunda ortaya çıkan anormal durumların tespitinde, sensör verilerindeki değişimler ve GPS değerlerindeki sapmalar üzerinde odaklanılmıştır. Bu faktörler, İHA'nın maruz kaldığı saldırıları tespit etmek için kullanılan önemli belirteçlerdir.

Literatürdeki çalışmalarda, İHA'lara yönelik saldırıların tespiti için farklı yöntemler ve stratejiler ele alınmaktadır. Anomali tespiti, İHA'nın normal uçuş ve çalışma durumlarına kıyasla beklenmedik davranışları veya veri değişikliklerini tespit etmek için kullanılan bir yaklaşımdır. Sensör verileri üzerinde yapılan analizler ve GPS değerlerindeki anormallikler, saldırılar veya dış müdahaleler sonucunda oluşan İHA'nın anormal durumlarını belirlemeye yardımcı olmaktadır.

Bu bölümde literatürdeki bazı çalışmaların incelenmesi sonucunda elde edilen bulgular üzerinde durulacak ve İHA'lara yapılan saldırıların tespiti ve engellenmesi için kullanılan yöntemlere değinilecektir. Sensör verilerinin analizi, yapay zekâ ve makine öğrenimi yöntemlerinin kullanımı, hava aracındaki arızalar ve anormalliklerin değerlendirilmesi gibi yaklaşımlar üzerinde durularak İHA'ların saldırılara karşı korunmasına yönelik ileriye dönük çalışmaların yol haritası çizilecektir.

Sedjelmaci ve arkadaşları [4] tarafından 2016'da yapılan çalışmada, insansız hava aracı (İHA) ağlarının güvenlik konularına odaklanılmış ve özellikle veri bütünlüğünü ve ağ erişilebilirliğini hedefleyen siber saldırılara karşı etkili bir siber güvenlik sistemi önerilmiştir. Bu önerilen sistemin temelini, hızlı siber tespit mekanizması ve İnanç yaklaşımına dayalı tehdit tahmini modeli oluşturmuştur. Ayrıca, yapılan simülasyonlar, bu önerilen güvenlik sisteminin mevcut literatürdeki siber tespit sistemlerine göre daha yüksek doğruluk oranlarına sahip olduğunu göstermiştir. Çalışmada, İHA sayısı arttıkça doğruluk oranı düşmesine rağmen tespit oranının %93'ten fazla, yanlış pozitif oranı ise %3'ten az olduğu ifade edilmektedir.

Muniraj ve Farhood [5] tarafından 2017'de yapılan çalışmada, küçük bir insansız hava aracı sistemi için hem siber hem de fiziksel katmanlardaki kötü niyetli saldırılara karşı dayanıklı, güvenli bir otomatik pilot tasarımı konusundaki genel çabanın bir parçası olarak ele alınmıştır. Bu makale özellikle, küçük bir UAS'ın sensörlerine yönelik kötü niyetli saldırıların belirlenmesi üzerine odaklanmaktadır. İstatistiksel analiz yöntemleri, olasılıksal bir yaklaşım kullanarak sensör saldırılarını tespit etmek amacıyla sunulan bir çerçeve içinde değerlendirilmiştir. Aynı zamanda, GPS üzerindeki sahtecilik saldırısının tespiti örneği, önerilen yaklaşımı açıklamak amacıyla makale boyunca kullanılmaktadır. Anomali tespit cihazları, bir simülasyon veri seti temel alınarak tasarlanmış ve küçük sabit kanatlı bir İHA platformunda gerçekleştirilen uçuş testleri sonucunda yeniden ayarlanmıştır. Bu detektörlerin performansı farklı dışsal müdahale koşulları altında incelenmiş ve sonuçlar çıkarılmıştır.

Zhu ve arkadaşları [6] tarafından 2018'de yayımlanan çalışmada, insansız hava araçlarının güvenliğine insan-özerk işbirliği yaklaşımının etkisi incelenmiş ve bu yaklaşımın potansiyelini ortaya koymuştur. Çalışmaları, birden fazla İHA'nın tek bir operatör tarafından denetlendiği senaryoda insanın coğrafi konumunu kullanarak siber saldırıları tespit etme başarısını vurgulamıştır Sonuç olarak yanlış alarm da başarı %84 iken gerçek bilgisayar korsanlığında başarı %78 civarında bulunmuştur.

Solodov ve arkadaşları [7] insansız hava araçlarının nükleer tesisler için oluşturduğu tehditleri ve önleme yöntemlerini ele aldıkları çalışmalarında, İHA'ların hem faydalı uygulamalarını hem de potansiyel risklerini detaylı bir şekilde incelemişlerdir. Bu çalışma ayrıca İHA'ların güvenlik olaylarına dair örnekleri sunarak, nükleer tesislerin İHA saldırılarına karşı nasıl korunabileceğini tartışmış ve gelecekteki araştırma alanlarına işaret etmiştir.

Renyu ve arkadaşları [8], İHA'ların GPS sinyalleri ile yönlendirildiği ve birbirleriyle iletişim kurabilen senaryolarda sahtecilik saldırısının gereksinimlerini ve farklı sahte sinyal sayılarıyla saldırının performansını inceledikleri çalışmalarında, ayrıca hücresel ağlar tarafından sağlanabilen OTDOA konumlandırması ile yönlendirilen İHA'lar üzerindeki sahtecilik saldırısını simüle ettikleri görülmektedir.

Sedjelmaci ve arkadaşları [9], İHA ağlarının güvenlik sorunlarını ele alan çalışmalarında, İHA ve yer istasyonu seviyelerinde çalışan yeni bir sızma tespit ve yanıt şemasını tasarlayıp uygulamışlardır. Bu şema, kötü niyetli anormallikleri tespit etmek için önerilen bir dizi teknik içermekte olup özellikle yanlış bilgi yayılması, GPS sahteciliği, sinyal karıştırma ve diğer siber saldırılara karşı koruma odaklıdır. Yapılan simülasyonlar, önerilen yöntemin büyük sayıda İHA ve saldırgan durumlarında bile yüksek tespit oranı ve düşük yanlış pozitif sayısı sağladığını göstermektedir.

Whelan ve arkadaşları [10], İHA'lar için zeki bir sızma tespit sistemi tasarımını ele aldıkları çalışmalarında, İHA'ların kablosuz protokollere dayalı işletim ortamlarında karşılaştığı geniş tehdit

yelpazesini incelemişlerdir. Çalışma, tek-sınıf sınıflandırıcılar kullanarak İHA'ların saldırıları tespit etme amacıyla bir yenilik tabanlı yaklaşım önermektedir. Tek-sınıf sınıflandırıcıların uygulanması ve değerlendirmesi, farklı İHA platformlarında etkili olduğunu ve özellikle GPS sahteciliği gibi harici sensör tabanlı saldırıları tespitte yüksek performans gösterdiğini göstermiştir.

Rahman ve arkadaşları [11], çalışmalarında donanım saldırıları sonucu kompromize edilmiş güç elektroniği elemanları üzerinden İHA'ların güvenliği ve güvenilirliğinin tehlikeye girebileceği vurgulanmıştır. Bu çalışma, makine öğrenimi tabanlı bir sızma tespit sisteminin (STS) güç elektroniği/mikrodenetleyici seviyesinde uygulanarak, donanım saldırılarına karşı başa çıkma amacını taşımaktadır.

Park ve arkadaşları [12] çalışmalarında, İHA'ların kontrol bileşenlerindeki hataların tespiti ve bu alandaki önceki yaklaşımları ele almışlardır. Kural tabanlı ve denetimli öğrenmeye dayalı yöntemlerin sınırlamaları ortaya konmuş, bu sınırlamaları aşmak için denetimsiz öğrenme altında çalışan bir otomatik kodlayıcı hata tespit modeli önerilmiştir. Çalışma, özellik çıkarmak için yapılan analizler, otomatik kodlayıcı ve sınıflandırıcı kullanımı ve farklı tipteki İHA hatalarıyla yapılan testler gibi temel katkıları sunmaktadır.

Davidoviç ve arkadaşlarının [13] çalışmasında, GPS sahtecilik saldırılarının mikro İHA'lar üzerindeki etkisini gerçek zamanlı olarak tespit etmek amacıyla İHA kamerasının yakaladığı video akışını kullanarak yenilikçi bir yöntem önerildiği belirtilmektedir. Önerilen yöntemin performansı hem simüle edilmiş uçuş ortamında deneylerle hem de gerçek dünyada bir DJI drone ile test edilerek incelenmiştir. Bu çalışma, GPS sahtecilik saldırılarına karşı farklı güvenlik seviyeleri sağlayabilen bir tespit yöntemi sunmaktadır.

Bu çalışmada, literatürde bulunan çeşitli makalelerin incelenmesi sonucunda elde edilen bulgular üzerinde durulacak ve İHA'lara yapılan saldırıların tespiti ve engellenmesi için etkili stratejiler sunulacaktır. Sensör verilerinin analizi, yapay zekâ ve makine öğrenimi yöntemlerinin kullanımı, GPS verilerindeki sapmaların değerlendirilmesi ve uçuşlarda yaşanan anormal davranışların değerlendirilmesi gibi yaklaşımlar üzerinde durularak İHA'ların saldırılara karşı korunmasına yönelik ileriye dönük çalışmaların yol haritası çizilecektir.

3. İHA'LARIN SINIFLANDIRILMASI, HABERLEŞMESİ VE İHA'LARA MÜDAHALE YÖNTEMLERİ

Günümüzde İHA'lar birçok alanda kullanılmaktadır. Kullanılan İHA'lar hobi, eğlence, doğa çekimleri, askeri, siber güvenlik, casus, tarımda tohumlama ve ilaçlama, yangın söndürme, kargo taşıma, baz istasyonları, insanların ulaşamadığı tehlikeli olan birçok alanda aktif olarak kullanılmaktadır. Türkiye'nin içinde bulunduğu jeopolitik konumundan dolayı birçok doğal afet gibi öngörülmesi zor olan koşullarda insanların acil ilaç, yardım çağrısı, haberleşme için seyyar baz istasyonlarına ihtiyaç duyulması gibi çok çeşitli alanlarda aktif olarak görev almaktadır.

3.1. İHA'ların Sınıflandırılması

İHA'lar farklı kullanım alanlarından dolayı yapısında birden fazla sensör ve cihaz barındırmaktadır. Bulunan bu sensörler ve cihazların ağırlıkları, işlevleri, boyutları, kullanım yerleri birbirlerinden farklı olduğundan çeşitli sınıflandırmalara tabi tutulmaktadır. İHA'ların içerisinde yer alan GPS (yer istasyonu), baz istasyonu, komuta merkezi, mühimmat içermesi veya içermemesi sınıflandırma etkenleri içerisinde yer almaktadır. Ağırlıklarına, yüksekliklerine, menzillerine, kanatlı veya rotorlu yapılarına ve uygulama alanlarına göre sınıflandırılmaktadır.

Tablo 3.1'de ağırlıklarına ve buna bağlı olarak farklı ehliyet gruplarına göre İHA sınıfları verilmiştir.

Tablo 3.1. Ağırlıklarına ve Ehliyet Türlerine göre İHA'lar

	Ağırlık (kg)	**İHA Ehliyet Türü**	**İHA Ehliyeti İçin Koşul**
Nano	0gr - 250gr	İHA 0	-
Mikro	250gr – 2kg	İHA 0	500gr - 4kg (İHA 0)
Küçük	2kg – 25kg	İHA 1	4kg – 25kg (İHA 1)
Orta	25kg – 150kg	İHA 2	25kg – 150kg (İHA 2)
Büyük	150kg - Üzeri	İHA 3	150kg – Üzeri (İHA 3)

Rakım ve menzil aralığına göre İHA'lar:

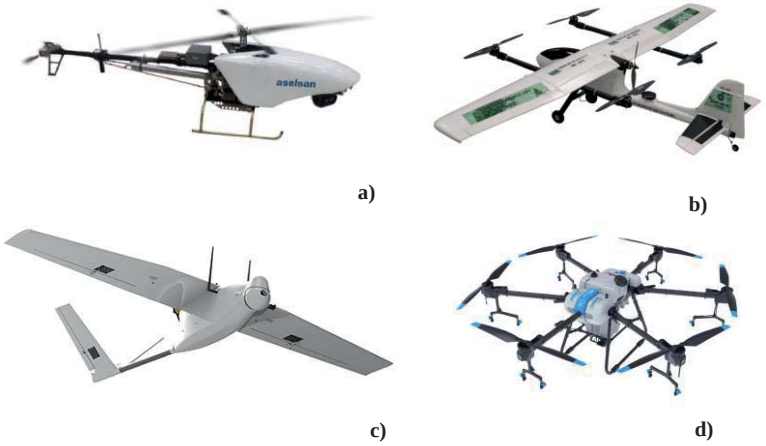
- El tipi: 600m'den daha düşük irtifada uçabilen ve menzili 2km'den az olan İHA'lar.
- Kapalı: 150m'den az irtifaya ve 10km'den daha az menzile sahip olan İHA'lar.
- NATO: İrtifası 3000m'den az ve menzili 50km'den az olan İHA'lar.
- Taktik: İrtifası 5550m'den az ve menzili 160km'den az olan İHA'lar.
- MALE (Orta irtifa uzun menzil): İrtifası 9100m'den az ve menzili 200km'den az olan İHA'lar.

- HALE (Yüksek irtifa uzun menzilli): İrtifası 9100m'den fazla ve belirsiz menzilli İHA'lar.
- Hipersonik: 15200m civarında olan ve menzili 200km'den fazla olan İHA'lar [14].

3.1.1. Kanat ve Rotorlara Göre İHA'lar

İHA'lar günümüzde birçok farklı alanda kullanılmakta ve alanlara özgü yapılarından dolayı dört farklı statüde değerlendirilmektedir.

- **Tek Rotorlu**: Bu tür İHA'ların üstünde bulunan bir ana rotoru ve kuyruk kısmında bulunan küçük bir rotoru olan, helikoptere benzeyen bir yapısı bulunmaktadır. Uçurulması diğer İHA'lara nazaran daha tehlikeli, zor ve eğitim alınması gerekmektedir. Genel manada uzun uçuş sürelerine sahip olup LİDAR taraması yapabilmektedirler. Şekil 3.1(a)'da tek rotorlu bir İHA'ya ilişkin görsel verilmiştir.
- **Sabit Kanatlı Hibrit VTOL**: Dikey kalkış ve iniş yapabilen sabit kanatlı İHA olarak kullanılmaktadır. Genel olarak sabit kanat ve döner kanat İHA'ların yapabildiği görevleri gerçekleştirebilmektedir. Askeri alanlarda pistin olmadığı ve uzun uçuş süreleri istenen olay örgülerinde kullanılmaktadır. Şekil 3.1(b)'de sabit kanatlar üzerinde dikey hareket kabiliyeti kazanabilmesi için tasarlanmış bir hava aracı görülmektedir.
- **Sabit Kanat**: Uçak görünümde olan ve uzun uçuş sürelerine sahip olan bir İHA modelidir. Genellikle askeri alanlarda, hava haritalama, boru ve enerji hatlarının korunması ve denetlenmesinde kullanılmaktadır. Şekil 3.1(c)'de uçak görümüne sahip bir hava aracı görülmektedir.
- **Çok Rotorlu**: Bu tür İHA'lar birden fazla rotoru bulunan ve en yaygın olarak kullanılan İHA sınıfıdır. En yaygın olan türleri: Quadcopters, hexacopters ve octacopters olarak bilinmektedir. Kısa uçuş süreleri olmakla birlikte zirai ilaçlama alanlarında, birçok film setinde, hobi amaçlı fotoğraf ve video çekme alanında yaygın olarak kullanılmaktadır. Şekil 3.1(d)'de altı döner rotora sahip bir hava aracının görseli verilmiştir.



Şekil 3.1. Kanat ve rotorlarına göre İHA türleri

3.1.2. Uygulamaya Dayalı Sınıflandırma

İHA'lar gün geçtikçe yaygınlaşan, insan hayatına hızlı bir şekilde giren ve üzerine entegre edilebilen sistemler ile beraber farklı amaçlara öncülük eden sistematik makineler haline gelmektedir. İHA'lar uygulama alanlarına göre aşağıdaki gibi sınıflandırılabilir:

- **Kişisel**: Kişinin kendine özgü, bireysel olarak uçurma izninin olduğu bölgelerde kendi zevk ve becerilerini geliştirmek adına uçurduğu hava araçları olup kişisel video çekimleri, eğlence amaçlı uçuşlar ve doğa çekimleri, drone yarışmaları gibi birçok alanda kullanılmaktadırlar.
- **Ticari**: Tarımsal ilaçlama ve tohumlama alanlarında, sinema sektöründe, alt yapı izlemede, konumlama ile arazi ölçümlerinin yapılmasında, ürün teslimi gibi görevlerde kullanılmaktadır.
- **Devlet ve Kolluk Kuvvetleri**: Yangın ile mücadele, orman arazilerinde tohumlama yapmada, kaçakçılık yapılabilen arazilerde insan tespiti, devriye atma gibi uygulamalarda kullanılmaktadır.
- **Askeri**: Gözetleme, muhabere saldırıları, doğalgaz ve enerji hatlarına yapılacak saldırı ve tehditler için gözetleme, ülke sınırlarının korunmasında ve birçok askeri alanda kullanılmaktadır.

Avrupa İnsansız Hava Sistemleri Kurumu'nun (EUROUVS) yaptığı askeri amaçlı İHA sınıflandırması Tablo 3.2'de verilmiştir. Ülkemiz bu alanda dünya sıralamasında ilk üç içerisinde yer almakta olup birçok keşif, takip ve imha görevlerinde aktif olarak bu İHA'lardan yararlanmaktadır. Bu alanlarda firma olarak öne çıkan Baykar tarafından üretilen Baykar Taktik İHA ve yine askeri birliklere teslim edilmesi beklenen Kızılelma insansız savaş uçağı gibi birçok hava aracının yapılması, ülkemiz adına gurur verici gelişmelerdir. Aynı zamanda Taktik MALE sınıfında TAİ (Türk Havacılık ve Uzay Sanayii A.Ş.) tarafından ANKA ve Vestel tarafından Karayel İHA'larının testleri başarıyla tamamlanmıştır ve askeri birliklere teslim edilmiştir.

Tablo 3.2. EUROUVS İHA sınıflandırılması [14] [15][16]

Kategoriler		Maksimum Kalkış Ağırlığı	Maksimum Uçuş Ağırlığı	Havada Kalma/Dayanama Süresi (Saat)	Veri Haberleşme Menzili (km)
Mikro/Mini İHA	Mikro	0.1	250	1	<10
	Mini	<30	150-300	<2	<10
	Yakın Menzil	150	3000	2-4	10-30
	Kısa Menzil	200	3000	3-6	30-70
	Orta Menzil	150-500	3000-5000	6-10	70-200
Taktik İHA	Uzun Menzil	-	5000	6-13	200-500
	Dayanımlı	500-1500	5000-8000	12-24	>500
	Orta İrtifa Uzun Havada Kalış (MALE)	1000-1500	5000-8000	24-48	>500
Stratejik İHA	Yüksek İrtifa Uzun Havada Kalış (HALE)	2500-12500	15000-20000	24-48	>2000
	Öldürücü	250	3000-4000	3-4	300
Özel Görev İHA	Tuzak	250	50-5000	<4	0-500
	Stratosferik	-	20000-30000	>48	>2000
	Ekzotosferik	-	>30000	-	-

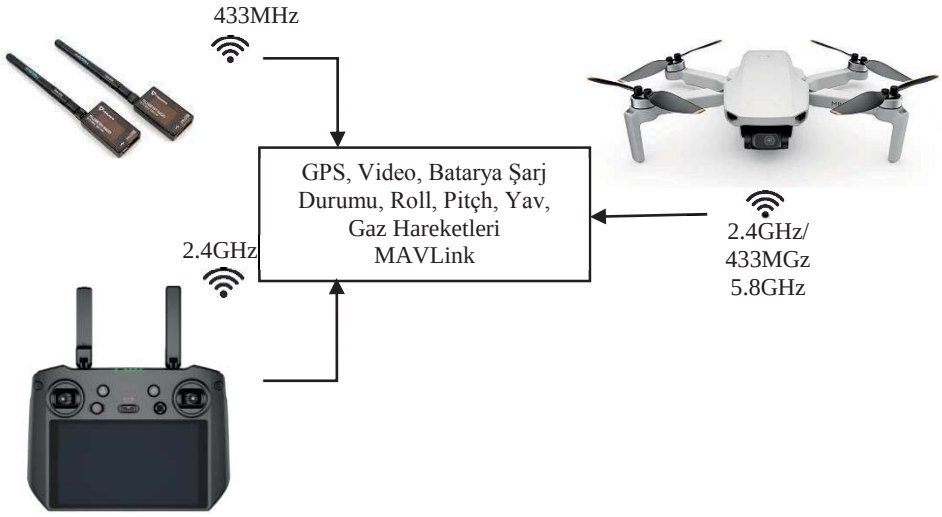
3.2. İHA'larda Haberleşme Yöntemleri

İHA'ların çalışabilmeleri ve görevlerini yerine getirebilmeleri için çeşitli kablosuz haberleşme teknolojileri kullanılmaktadır. Kullanılan teknolojik araçlar görev, faaliyet ve kullanım yerlerine göre değişiklik göstermektedir. İHA'larda kullanılan kablosuz haberleşme teknolojileri şunları içermektedir:

- Radyo Frekansı (RF)
- Bluetooth
- Wi-fi
- 3G/4G/LTE (4.5G)
- Uydu
- GPS

3.2.1. Radyo Frekansı Üzerinden Haberleşme

Radyo frekansı üzerinden haberleşen hava araçları genellikle hava araçlarının hareketi, kamera açılarındaki hareket, video alıcı ve video verici gibi haberleşmeler için 900MHz, 1.2-1.3GHz, 2.4GHz, 5.8GHz frekanslarını kullanmaktadırlar [17]. Bildiği üzere frekans ne kadar düşük ve dalga boyu ne kadar uzun olursa nüfuz etme gücü o kadar büyük olmaktadır. Ancak



Şekil 3.2. İHA'larda radyo frekansı üzerinden haberleşme

bununla birlikte antenin fiziksel boyu da orantılı bir şekilde büyük olmaktadır. Bunun içinde belirlenen frekanslar hava araçlarına entegre edilebilecek boyutlu olanlara göre seçilmektedir. Genellikle video akışı için düşünülen 5.8GHz'lik frekanslar kullanılmaktadır. Buna bağlı olarak tarım ilaçlama, felaket kurtarma, manzara çekimleri, yangın tespiti gibi birçok göreve sahip olan hava araçları için 2.4GHZ ve/veya 5.8GHz frekansları kullanılmaktadır. Bazı hobi ve ticari amaçlı üretim yapan firmalar, tek frekans üzerinden hem video akışı hem de hava aracının kontrolünün yapıldığında çeşitli problemler yaşandığını görülmektedir. Şekil 3.2'de radyo frekansı ile haberleşen bir İHA modeli görülmektedir.

3.2.2. Bluetooth ve Wi-fi Haberleşmesi

Bluetooth genelde kısa mesafeler için kullanılan haberleşme yöntemlerinden biri olmaktadır. Bu kısa mesafeden dolayı genelde hobi amaçlı kullanımlarda daha sık rastlanılmaktadır. Yaklaşık menzil olarak bakıldığında basit düzeyde ve ucuz olan modellerinde 20m civarında bir menzile sahip oldukları görülmektedir. Bunun yanı sıra geliştirilmiş Bluetooth teknolojisi ile birlikte Bluetooth 4.2 çift mod modülü ise 500m – 1000m arasında bir menzile sahip olup harici kamçı anteni kullanarak bu mesafe yaklaşık olarak 2000m'ye çıkartılabilmektedir.

Wi-fi haberleşme teknolojisi Bluetooth'a nazaran daha uzun mesafeler için kullanılmaktadır. Tercih edilen basit ve ucuz olan modüllerin menzili 50m civarında olduğu göz önünde bulundurulduğunda genel manada bu haberleşme modülü için hobi amaçlı kullanımların daha yaygın olduğu görülmektedir. Gelişen Wi-fi teknolojisi ile beraber son yıllarda haberleşme mesafesi de bariz bir biçimde artmıştır. Wi-fi modülü olan RDF 900X uzun mesafeli telemetri modülünün kapalı alanda 500m – 1000m aralığında açık alanda da antene bağlı olarak 40km'ye

yakın bir menzilinin olduğu görülmektedir. Şekil 3.3'te temsili olarak Wi-fi haberleşme yapısı gösterilmektedir.

Şekil 3.3. İHA'larda Wi-fi haberleşemesi

Gün geçtikçe gelişen teknoloji ile Wi-fi ve Bluetooth menzilleri arttığından kullanım alanları da artmaktadır. Wi-fi genel manada görüntü aktarımı konusunda tercih edilen bir yöntem olarak kullanılmaktadır.

3.2.3. 3G, 4G, LTE (4.5G) Haberleşmesi

3G, 4G, LTE, gelişmekte olan 5G teknolojisi, internet ve cep telefonu baz istasyonunun internet servis sağlayıcı altyapısını kullanmaktadır. Bu servis ağlarının nihai maksadının başında video akışını daha net bir şekilde alıp hızlı karar verebilmesi yer almaktadır. Gelişmekte olan 5G teknolojisi ile video akışını gerekli ekipmanlarla hava aracını kullanan kişiye kesintisiz ve yüksek çözünürlükte iletmektedir. Otonom olarak görevlendirilen hava aracının, daha hızlı karar veren ve sonuca ulaşmasını hedefleyen haberleşme yöntemleri arasında yer almaktadır. Son zamanlarda artan doğal afet ve orman yangınlarında, daha hızlı ve etkili müdahalede bulunmakta kullanılmaktadır. Ayrıca yangın büyümeden yangının kaynağının belirlenmesinde etkin bir rol oynamaktadır.

3.2.4. Uydu ve GPS Haberleşmesi

Uydu haberleşmesi, genel olarak MALE (orta irtifa uzun havada kalış) ve HALE (yüksek irtifa uzun havada kalış) gibi askeri amaçlı kullanılan yüksek menzilli ve uzun süre havada kalabilen hava araçları için kullanılmaktadır. Haricen İHA'lara yapılan saldırılar neticesinde İHA ile yer kontrolü arasındaki görüş hattı kesildiğinde aralarındaki iletişim uydu üzerinden yapılabilmektedir [18].

Küresel konumlama sistemi GPS, Amerika tarafından geliştirilen, ilk maksadı askeri kullanım için olan, konum bilgisini alarak haberleşme sağlayan teknolojidir. GPS askeri alanlarda takip, saldırı, gözetleme ve keşif gibi amaçlarla kullanıldığı gibi sivil insanlar için de hayatı kolaylaştırmaktadır.

3.3. İHA'lara Müdahale Yöntemleri

İHA'ların özel ve askeri olmak üzere birçok sektörde kullanıldığı bilinmektedir. Kullanım alanlarından biri olan hassas tarım yapan Drone'un öncelikli işi, tarım yapılacak bölgeyi ilaçlama, tohumlama, gübreleme ve toprak verim analizi gibi faaliyetleri bulunmaktadır. Bu faaliyetler için minimum ağırlık olarak 10kg'lık, maksimum 60kg'lık bir Drone'dan bahsedildiğinde, bu Drone'lara yapılacak saldırının neticesinde yakınlarında bulunan fabrika, işyeri, protokol yolu, baz istasyonu veya yerel halkın bulunduğu bölgelere saldırı düzenlenmesi bir felaket ile sonuçlanabilecektir. Bunun yanı sıra Drone'nun kaçırılması sonucunda maddi hasar da çok fazla olacaktır. Yangın tespit Drone'larına herhangi bir saldırı gerçekleştirilmesi yangının konum verilerinin ve şiddetinin yanlış verilmesi durumunda hektarlık arazilerin ve ormanların yok olmasıyla sonuçlanabilecektir. Bir film setinde Drone'larla yapılan çekim esnasında yapılacak siber saldırılar ile oyunculara suikast düzenlenmesi söz konusu olabilir.

Bunun yanı sıra İHA'lar askeri alanlarda sınır dışı operasyonlarda, ülkenin kendi sınırları içerisindeki gözetlemelerde, taarruzlarda, terör gruplarının yer bilgisinin alınmasında ve buna benzer birçok alanda kullanılmaktadır. Bu teknolojiye saldırı düzenlenmesi askeri anlamda mağlup olmaya neden olabilir.

İHA'lar terör gruplarına sağlanan bir teknoloji olduğunda, kimyasal gaz salınımı, suikast, nükleer santrallere saldırı, enerji hatlarına saldırı gibi birçok kötü niyetli amaçlar içinde kullanılabilmektedir. Buna benzer saldırılara karşı müdahale edebilecek yöntemler geliştirilmeye çalışılmaktadır.

Kötü amaçlar için kullanılan İHA'lara karşı kullanılan bazı müdahale yöntemleri aşağıda belirtilmiştir. Bu müdahale yöntemlerinden birkaçı görsel olarak Şekil 3.4'te verilmiştir.

- Müdahale amacıyla tasarlanmış İHA'lar
- Çarpışan İHA

- Özel yetiştirilmiş yırtıcı kuşlar
- Ateşli silahlar
- Kinetik enerji sistemleri (Mühimmat)
- Sinyal engelleyici (jammer)
- RF karıştırma
- Köreltme
- Küresel uydu seyrüsefer sistemi karıştırma (GNSS)
- Yanıltma sinyali (spoofing)
- Yüksek güçlü mikrodalga (HPM)
- Siber saldırı (Hack)
- Çoklu müdahale sistemleri

3.3.1. Müdahale Amacıyla Tasarlanmış İHA'lar

Müdahale amacıyla tasarlanmış İHA'ların yasaklı bölgede uçuş yapan veya tehdit olarak algılanan hava araçlarının etkisiz hale getirebilmesi için iyi eğitimli bir pilot tarafından kullanması gerekmektedir. Bu yöntemde, etkisiz hale getirilecek hava aracında zararlı bir madde bulunması durumunda müdahale eden hava aracının da zarar görmesi muhtemeldir. Bu yöntemin en büyük dezavantajı iyi eğitilmiş, kalifiye pilot yetiştirilmesi gerekliliğidir.

3.3.2. Çarpışan İHA

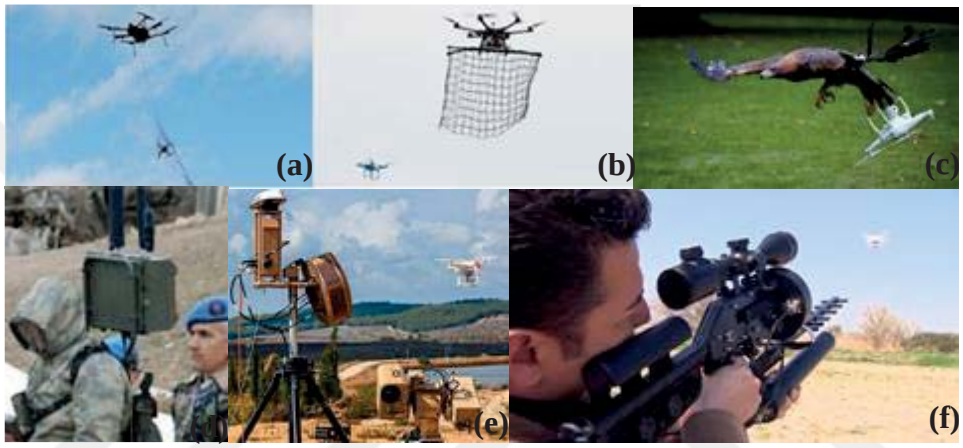
Çarpışan İHA yöntemi, basit ölçekli İHA'ların düşük maliyetli olmasından dolayı tercih edilen bir yöntemdir. Saldırı önleme sistemi kendini imhaya yönelik bir sistem olduğundan bu yöntemin şehir içi ve insanların yoğun olduğu yerlerde kullanılması uygun olmamaktadır. İnsan yaşamını tehlikeye sokması ve maddi kayıplara neden olması bu yöntemin uygulama alanlarını kısıtlamaktadır.

3.3.3. Özel Yetiştirilmiş Yırtıcı Kuşlar

Özel yetiştirilmiş yırtıcı kuşlar eğitmenlerin ödül ve ceza yöntemleri sonucunda kartal, atmaca veya şahin gibi kuşları yetiştirerek küçük boyuttaki İHA'ları etkisiz hale getirmeyi hedeflemektedir. Yırtıcı kuşlar doğaları gereği havada uçan kuşları yakalayıp etkisiz hale getirdikleri gibi küçük İHA'ları da benzer şekilde etkisiz hale getirebilmektedir. Şekil 3.4(c)'de özel olarak eğitilmiş yırtıcı bir kuşun hedef olarak gösterilen bir insansız hava aracını nasıl etkisiz hale getirdiği görülmektedir.

3.3.4. Ateşli Silahlar

Ateşli silahlarla müdahale yöntemi diğer metotlara nazaran daha az ve zayıf etki alanına sahiptir. Bu yöntem genelde fark edilmesi zor durumlarda ayırt edip diğer müdahale yöntemlerinin olmadığı askeri durumlarda karşı tarafın bilgi toplamasını ve saldırı gerçekleştirmesini önlemek için kullanılmaktadır. Bazı hobi amaçlı uçurulan ve özel mülkün ihlal edilmesi sebebiyle mülk sahibinin ateşli bir silah yardımıyla hava aracını düşürüp etkisiz hale getirmesi de bu önleme yöntemine örnek olarak gösterilebilir.



Şekil 3.4. İHA'lara müdahale yöntemleri.

3.3.5. Kinetik Enerji Sistemleri (Mühimmat)

Kinetik enerji sistemleri (mühimmat) daha çok özel tasarlanmış mühimmat ve silahlarla belirlenen İHA'yı vurmayı hedeflemektedir. Bu tür İHA sistemlerinde ayrıntılı balistik hesaplama gerekmektedir. Hava aracına monte edilmiş silahın ağırlığı, silahın kapasitesi, silahın geri tepme oranı gibi hesaplamalar yapılması gerekmektedir. Yapılan deneme atışlarında küçük ölçüdeki İHA'ların vurulma oranının çok az olduğu bilinmektedir.

3.3.6. Sinyal Engelleyici (Jammer)

Sinyal engelleyici (jammer) askeri uygulamalarda, mitinglerde, toplu etkinlik alanlarında, konserlerde kısacası insanlar için tehdit unsuru oluşturabilecek bölgelerde kullanılmaktadır. Bu yöntem ile sivil insanlara zarar vermek için uzaktan kumanda ile düzenlenen birçok saldırının ve terör eylemlerinin gerçekleştirilmesi önlemektedir. Bu gibi terör eylemleri genel olarak GPS, GSM ve radyo bağlantısını engellemek yoluyla etkisiz hale getirilebilmektedir.

3.3.7. Radyo Frekans Karıştırıcı (RF)

Radyo frekansı karıştırma (RF) sistemleri, büyük ölçüde sinyal engelleyicilerin (jammer) çalışma prensibinden etkilenerek yapılmıştır. Bu teknoloji İHA sistem savar üreticileri tarafından en çok üretilen ve askeriyeye en çok satılan teknolojiler arasında yer almaktadır. Bu sistem operatör ile İHA arasındaki haberleşme ağının karıştırılması veya kesilmesi mantığıyla çalışmaktadır. Eğer İHA'lar arasındaki bağlantı koparsa daha önceden belirlenen geri eve dön veya yavaşça bağlantının kesildiği noktaya doğru iniş yap komutu çalışmaktadır. Ancak sistem otonom İHA'lara karşı etkisiz kalmaktadır.

3.3.8. Köreltme

Köreltme sisteminin çalışma prensibi, İHA'ların kameralarına lazer veya yüksek ışık demeti gönderilerek görme yetilerinin engellenmesine dayanmaktadır [19]. İHA'lar gözetleme, keşif, haritalama gibi birçok bilgiyi alarak uygulayacakları operasyon faaliyet alanlarının analizini daha net bir şekilde yapmak için yüksek çözünürlüklü kameralardan yararlanmaktadırlar. Bu sistem sadece kameralar üzerinde etkili olduğundan İHA'nın tamamen etkisiz hale getirilmesi için yeterli değildir.

3.3.9. Küresel Uydu Seyrüsefer Sistem Karıştırma (GLONASS)

Küresel uydu seyrüsefer sistemleri ile karıştırma ve yanıltma sinyali oluşturma konularında yapılan çalışmalar birbirine çok benzemektedir. GPS ve GLONASS uydularından sinyallerin kesilmesi ve bu sinyallerin gösterdiği konumların belirtilenden farklı olması alınan önlemler arasında yer almaktadır. Sinyal kesilmesi İHA'nın kalkış noktasına geri dönmesi veya sinyalin kesildiği noktada yere inmesi ile sonuçlanır. Eğer aldatma (spoofing) durumu söz konusuysa İHA istenilen konumun haricinde yanlış bir konumu doğru konum olarak algılayabilir.

3.3.10. Yüksek Güçlü Mikrodalga (HPM)

Yüksek güçlü mikrodalga (HPM) sistemi, tasarlanan yüksek enerji dalgalarının İHA'lara yöneltilerek İHA'nın içindeki elektronik sistemleri etkisiz hale getirmekte ve böylelikle İHA'nın kontrolünü kendisi sağlamaktadır. HPM enerjisi, İHA içerisinde bulunan yarı iletkenlerin aşırı yüklenmesine, sistem karalılığının bozulmasına ve hatta bu elemanların yanmasına neden olabilmektedir.

3.3.11. Siber Saldırı (Hack)

Siber saldırı (Hack) ile etkisizleştirme yöntemi yukarda sayılan birçok yöntemin aksine maliyetsiz olması sebebiyle tercih edilmektedir. Bu yöntem kullanılarak İHA'ların haberleşme protokollerinde bulunan şifreli haberleşme kanallarının ve askeri kanallar için ayrılmış şifreli uydu kanallarının kırılması ile saldırılar gerçekleştirilmektedir. Bu saldırıları önlemek için karşı bir siber saldırı algılama sistemi geliştirilmelidir.

3.3.12. Çoklu Müdahale Sistemleri

Çoklu müdahale sistemleri yukarıda sayılan müdahale yöntemlerinden birden fazlasının bir arada kullanılması durumudur. Genelde siber saldırı yöntemi ile beraber RF karıştırma ve GNNS karıştırma özellikleri bir arada kullanılarak yapılmaktadır.

3.4. İHA'lara Yönelik Başlıca Siber Tehditler ve Saldırılar

İHA'lar gün geçtikçe gelişen ve birçok alanda kullanıma açılmış bir teknoloji olarak görülmektedir. Bu gelişen teknoloji güvenlik problemlerini de beraberinde getirmektedir. İHA'lar kablosuz haberleşme teknolojisini aktif olarak kullanmaktadır. Bu nedenle İHA'lara müdahale etmek amacıyla kablosuz haberleşme sistemlerine siber saldırılar düzenlenebilmektedir. Örneğin GPS sahtekârlığı veya yanlış bilgi yayma saldırıları nedeniyle planlanan görevin istenmeyen bir biçimde sonuçlanması durumu söz konusudur. Saldırının gerçekleşmesi ve başarıya ulaşması, o sistemde güvenlik açığı olduğu anlamına gelmektedir.

İHA'larda donanım ve iş yapabilme kapasitesi geliştikçe güvenlik açıkları da her geçen gün artmakta ve gelişen saldırılara yönelik yeni saldırı sistemleri geliştirilmektedir. En yaygın kullanılan saldırı türleri şunlardır:

- Yanlış bilgi yayma saldırıları
- Hizmet reddi (DoS) saldırıları
- Karıştırma saldırıları
- Gri delik ve kara delik saldırıları
- Güç elektroniği saldırıları
- İMU sahtekârlığı
- GPS sahtekârlığı

3.4.1. Yanlış Bilgi Yayma Saldırıları

Yanlış bilgi yayma saldırıları, hava araçlarına siber saldırılar düzenlenerek doğru olan bilgi ile doğru olarak kabul edilmesi istenen bilginin yer değiştirilmesidir. Kısacası doğru bilgi yerine

yanlış bilgi yönlendirilmektedir. Örnek verilecek olursa yangın söndürmek için görevlendirilen bir İHA'ya o bölgede yangın olmadığı bilgisinin gönderilmesi yangının büyümesine neden olabilmektedir. Buna benzer şekilde askeri amaçlı kullanılan İHA'lara sızılarak konum bilgisinin veya askeri mühimmatın bırakılacağı yerin yanlış verilmesi neticesinde istenmeyen sonuçlarla karşılaşılabilmektedir.

3.4.2. Hizmet Reddi (DoS)

Hizmet reddi (DoS) saldırıları, İHA'ların enerji kaynaklarını tüketmeye veya ağ ve yönlendirme protokollerini bozmaya çalışmaktadır [9]. İHA'larda enerji tüketimini artıracak birçok sensörün aktif edilerek gereksiz enerji tüketiminin sağlaması ve aynı zamanda İHA'nın yanlış yönlere yönlendirip tekrardan kendi istikametine sokulması planlanan görevin başarısız olmasına neden olmaktadır. Bu tip saldırılar, İHA'nın düşürülmesine veya kaçırılmasına neden olabilmektedir.

3.4.3. Karıştırma Saldırıları

Karıştırma saldırıları, hava aracının kumanda edildiği yer ve İHA arasındaki iletişimi bozmaya çalışmaktadır. GPS sahtekârlığına benzer bir şekilde GPS navigasyon sinyallerinin Drone'a ulaşmasını engellemektedir [9, 20, 21]. Bu saldırının asıl amacı hedef olan Drone'nun kontrolünün ele geçirilebilmesidir.

3.4.4. Güç Elektroniği Saldırıları

Güç elektroniği saldırıları, hava araçlarındaki kontrol kartlarına, motorlara, GPS donanımına, bataryalara ve buna benzer birçok elektronik bileşene yönelik olarak kullanılmaktadır. Bu bileşenlerin aşırı yüklenmesi uçuş kontrol kartına gelen veride yanlış bilgiye neden olmakta veya uçuş kartının devre dışı kalmasına sebep olabilmektedir. Bu sistemlere yapılan saldırılar hava aracının düşürülmesine veya yanlış sensör verilerinin alınmasına sebep olmaktadır.

3.4.5. İMU Sahtekârlığı

Yeni Nesil Navigasyon Sensör (İMU) sahtekârlığına bakıldığında kısmen güç elektroniği saldırılarına benzediği görülmektedir. İMU sensörü hava aracının doğrusal ve açısal hareketi ile ilgili bilgileri veren, içerisinde ivmeölçer ve jiroskop barındıran bir devre kartı olarak bilinmektedir. İMU sensörüne yapılan saldırılarda manevraya göre hava aracının davranışını değiştirerek kontrol sistemine geri bildirim olarak gönderilebilmektedir. Gönderilen aldatıcı bilgi neticesinde hava aracı beklenenin dışında bir manevraya zorlanarak etkisiz hale getirilebilmektedir.

3.4.6. GPS Sahtekârlığı

GPS alıcısının ürettiği konum bilgisi doğrultusunda hava aracının nerede ve ne kadar yükseklikte olduğuna dair bilgiler elde edilmektedir. Bu bilgilere saldırılması durumunda konum verileri doğru olmadığından İHA kontrolörünün aracı istenilen yere indirmesi mümkün olmayacaktır. Hatta saldırıyı düzenleyen kişiler sahte GPS sinyalleri yoluyla hava araçlarını ele geçirerek istedikleri yerlere saldırı düzenleyebilmektedir. 2011 yılında askeri bir İHA'nın İran ordusu tarafından ele geçirilmesi olayının böyle bir saldırı sonucunda olduğu iddia edilmektedir [22]. GPS sahtekarlığı diğer saldırı türleri arasında en yaygın olarak kullanılan saldırı türüdür.

3.5. İHA Saldırı Tespit Sistemleri

Saldırı tespit sistemi (STS) ya da izinsiz giriş tespit Sistemi (IGTS) genel manada bilgisayar ağları ve sistemlerinde olası kötü niyetli veya zararlı aktiviteleri tespit etmek için kullanılan bir güvenlik mekanizması olarak tanımlanabilmektedir. IGTS'ler ağ trafiği, sistem günlükleri, uçuş günlükleri ve diğer veri kaynakları üzerinde analiz yaparak potansiyel saldırıları veya ihlalleri belirlemeye ve tespit etmeye çalışmaktadır.

IGTS'lerin temel amacı ağa veya sistemlere yönelik saldırıları tespit etmek ve bunlara yönelik hızlı bir şekilde tepki verebilmek, böylece potansiyel zararın önlenmesi sağlanmaktadır. Genel manada IGTS'ler dört ana başlıkta sınıflandırılmaktadır.

3.5.1. Spesifikasyona Dayalı IGTS

Spesifikasyona dayalı IGTS'ler, İHA'ların beklenen davranışlarına dayalı olarak belirtilen ilgili kurallarla birleştirilmektedir. Bu birleştirilen kurallar, İHA sistemlerinin normal uygulamalarını izlemek için kullanılmaktadır [23] [24]. Spesifikasyon tabanlı tespit, sistem veya ağın normal davranış modellerini belirler ve bu normal davranışlardan sapmaları tespit ederek anormal aktiviteleri belirlemeye çalışır. Bu yaklaşım yeni ve özgün saldırıları yakalama konusunda daha esnek olabilir, çünkü saldırganlar sürekli olarak taktiklerini değiştirirken bile belirli davranış kalıpları dışındaki anormallikleri tespit edebilir. Bu yaklaşım, sadece önceden bilinen saldırı imzalarına bağlı olmadan geniş bir saldırı yelpazesini tespit etmeye çalışabilir. Bu nedenle, bilinmeyen veya önceden tespit edilmemiş saldırıları bile algılama potansiyeline sahip olabilir.

3.5.2. İmza Tabanlı IGTS

İmza tabanlı IGTS yöntemi, önceden tanımlanmış imzalara dayalı bilinen saldırıları tespit etmeyi amaçlamaktadır [25]. İmza tabanlı IGTS'lerin spesifikasyona dayalı sistemlerle yakından ilişkili olduğu görülmektedir. İmza tabanlı sistemler, bilinen saldırı imzalarını içeren bir veri tabanını kullanarak saldırıları tespit etmektedir. İmzalar, saldırgan aktivitenin karakteristik

özelliklerini temsil eden desenler veya dizi biçimindeki veriler olarak kullanılmaktadır. Bu imzalar, bilinen saldırıları tanımlayan belirli bir dizi bayt veya karakterler olarak ifade edilmektedir. İmza tabanlı sistemler, ağ trafiğini veya sistem günlüklerini izleyerek imza veri tabanındaki imzalarla eşleşen aktiviteleri tespit etmektedir. Eşleşen bir imza bulunduğunda, bir saldırı veya kötü niyetli aktivite olduğuna dair bir alarm üretilmektedir. Bu sistemler, yaygın olarak kullanılan saldırıların tespitinde etkilidir. Bu nedenle yeni veya değiştirilmiş saldırıları tespit etmek için imza veri tabanının sürekli olarak güncellenmesi gerekmektedir. Aksi takdirde, bilinmeyen veya önceden tanımlanmamış saldırılar sistem tarafından tespit edilememektedir.

3.5.3. Anormallik Tabanlı IGTS

Bir sistemde gözlemlenen bir arıza, saldırı veya anormal bir durumda anormallik davranışı tespit edilmektedir. Bu yöntem, bilinen veya bilinmeyen saldırıları tespit etmek amacıyla önceden tanımlanmış imzaların olmadığı (bilinmeyen) saldırıların tespitini büyük ölçüde artırabilen bir öğrenme mekanizması olarak kullanmaktadır [26].

Anormallik tabanlı IGTS'ler, normal ağ trafiği davranışını analiz ederek anomali veya istisnai durumları tespit etmeye odaklanmaktadır. Bu sistemler, bir ağdaki normal davranış modellerini öğrenerek çalışmaktadırlar. İlk olarak, normal ağ trafiği, kullanıcı aktiviteleri, ağ protokolleri ve sistem davranışları gibi unsurları analiz etmekte ve bunları bir normal davranış profili olarak öğrenmektedir. Daha sonra, gerçek zamanlı olarak ağ trafiğini izlemekte ve önceden öğrenilen normal davranış modeliyle karşılaştırmaktadır. Eğer tespit edilen trafiğin normal davranıştan sapma gösterdiği belirlenirse, bir anormallik veya olası bir saldırı girişimi olarak işaretlenir ve bir alarm üretilmektedir. Spesifikasyon tabanlı tespit sistemi önceden belirlenmiş davranış modellerine dayanırken, anormallik tabanlı tespit sistemi genel olarak normallikten sapmaları belirlemeye çalışır. İkinci yaklaşım, özellikle bilinmeyen veya özgün saldırıları yakalamak için daha uygundur, ancak daha fazla yanlış pozitif uyarıya yol açabilir.

3.5.4. Hibrit IGTS

Hibrit yöntem, hem bilinen hem de bilinmeyen saldırıları yakalayabilen yani hem imza tabanlı hem de anormallik tabanlı sistemleri kullanabilmektedir [27]. Bu sistemler, her iki yöntemin avantajlarını bir araya getirerek daha güçlü ve esnek bir tespit yeteneği sunmayı hedeflemektedir. İmza tabanlı yaklaşım, bilinen saldırı imzalarını tespit ederken, anormallik tabanlı yaklaşım da bilinmeyen veya önceden tanımlanmamış saldırıları tespit eder. Bu şekilde, hibrit IGTS geniş bir koruma sağlayabilmekte ve yeni saldırı kalıplarını da algılayabilmektedir. Daha az yanlış pozitif alarm durumu oluşabilmektedir. Sadece spesifikasyona dayalı veya imza tabanlı bir IGTS kullanıldığında, normal değişiklikler veya istisnalar yanlış pozitif alarmlara neden olabilmektedir.

Anormallik tabanlı yaklaşım, normal davranış modellerini analiz ederek bu tür yanlış alarmları azaltmaya yardımcı olabilmektedir. Bu sayede hibrit IGTS, daha kesin ve güvenilir bir tespit sağlamaktadır.

4. METODOLOJİ

Bu tez çalışmasında, gerçek uçuş günlüklerini barındıran ve bu uçuş günlükleri arasında da planlanmış arızalı uçuş günlükleri bulunan bir veri setinden yararlanılmıştır. Bu arızalı uçuş verileri imza tabanlı IGTS yerine anormallik tabanlı tek sınıflı IGTS sistemleri kullanılarak eğitilmiştir. Kullanılan veri setinde sabit kanatlı bir hava aracında oluşabilecek arızlar verilmiş olup, bu arızaların hava aracına saldırı neticesinde oluşabilecek anormal davranışlar olduğu kabul edilmiştir. Bu arızalı veriler anormallik olarak adlandırılmaktadır. Bu bölümde, referans alınan veri setinin nasıl eğitileceğine, hangi donanım özellikleri ile bu veri setinin elde edildiğine ve arıza durumlarına değinilmektedir.

4.1. İHA Donanımı

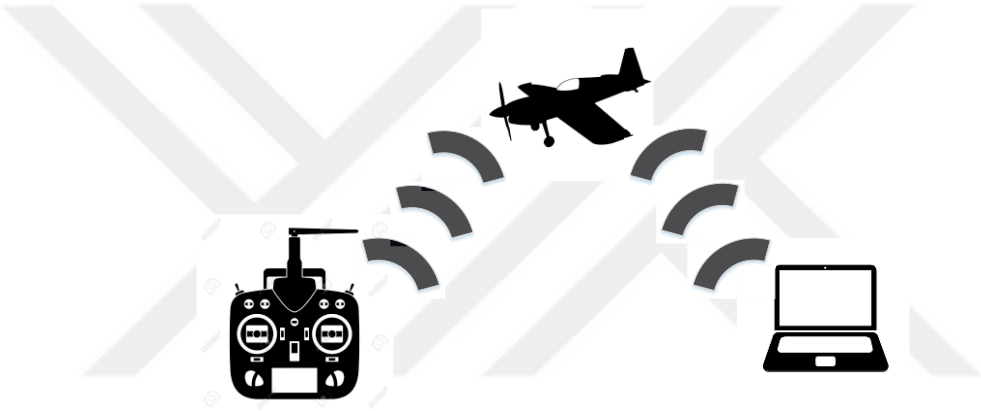
Veri setini toplamak için kullanılan hava aracı Carbon-ZT-28 model uçağının özel bir modifikasyonudur. Uçağın 2m kanat açıklığı, önde tek elektrik motoru, kanatçıkları, flaperonları, yukarı aşağı hareketini sağlayan arka kantlardaki asansörü ve dönüş için kullanılan dümeni bulunmaktadır. İnsansız hava aracı Holybro PX4 2.4.6 otopilot, pitot tüpü (hava hızı ölçümleri için), GPS modülü ve Nvidia Jetson TX2 yerleşik bilgisayarı ile donatılmıştır. Alıcıya ek olarak yer istasyonu ile iletişim için bir telemetry radyo frekansı alıcı ve vericisi ile bulunmaktadır [28]. Bu özelliklere sahip hava aracı Şekil 4.1'de görülmektedir. Pixhawk izleme için istenen verileri yayınlamak ve otonom bir uçuşta aktüatörlere arıza empozeetmek için değiştirilmiş Ardupilot/Arduplane v3.9.0 uçuş kontrol yazılımı kullanılmıştır [29].

Şekil 4.1. Yerleşik Bilgisayar ve Ek Modüler ile Donatılmış Carbon-ZT-28 Modelli [28].

Kullanılan bu ArduPlane güvenlik amacıyla aktüatörlerin yalnızca uçuş modu değiştirilene kadar çalışmaktadır. Bu yöntem pilotun tehlikeye gireceği herhangi bir zamanda hava aracının kontrolünü ele alma olanağı sağlamaktadır.

4.1.1. Veri Seti Oluşturmak için Kullanılan Otopilot Yazılımı

Oluşturulan veri setini elde edebilmek için anomali durumlarının oluşturulması ya da hava aracının havada sürekli bozulması gerekmektedir. İkinci yöntem hem insan ve çevre sağlığının tehlikeye girmesine hem de maliyetin artmasına neden olduğu için arızalar otopilot yardımı ile oluşturulmuştur. Pixhawk otopilot hava aracını hem otonom hem de manuel modlarda kontrol edebilmektedir. Kontrol ve simülasyonları gerçekleştirmek için Ardupilot/ArduPlane aygıt yazılımının özel bir sürümü kullanılmaktadır.



Şekil 4.2. İHA ve Yer İstasyonu Arasındaki İletişim (Pilot yalnızca görevi tehlikeye gireceği zaman devralmaktadır.)

Arıza durumlarını İHA'ya enjekte etmek için aşağıdaki fonksiyonlar kullanılmaktadır:

DisableEngine: Bu parametre, tam bir motor arızası simüle etmek için motoru devre dışı bırakabilmektedir.

DisableElevator: Bu parametre, sıkışmış bir asansörü (yukarı aşağı hareketi) engellendiği için yatay konumda sabitleyebilmektedir.

DisableRudder: Dümeni zorlama simülasyonu yapabilmektedir. Dümeni tamamen sağda, tamamen solda ya da ortada sabitleyebilmektedir.

DisableAileron: Sıkışmış kanatçıkları simüle etmek için sağ kanatçık, sol kanatçık veya her ikisini de yatay konumda sabitleyebilmektedir [28].

Bu komutlar kullanılarak oluşturulan kontrollü arızalardan elde edilen veriler toplanarak veri seti oluşturulmuştur. Planlı bozcu girişler sayesinde güvenli uçuş yapılabilmekte ve olası tehlike durumları için senaryolar oluşturulabilmektedir.

Güvenlik nedeniyle, gerçekleştirilen planlı arızalar yalnızca otonom modda çalışacak şekilde programlanmıştır. Otonom uçuş sırasında pilot herhangi bir zaman aralığında kontrolü devralabilir veya arızayı tamamen devre dışı bırakabilmektedir. Devre dışı bırakıldıklarında hareket mekanizması ve motorlar tekrardan normal hale gelmektedirler. Bu devre dışı bırakma kontörlü yalnızca yer kontrol istasyonu tarafından gerçekleştirilmektedir. İHA ile yer istasyonu arasındaki iletişim temsili olarak Şekil 4.2'de gösterilmiştir.

Yer istasyonu için oluşturulan bilgisayar sisteminde Robotik İşletim Sistemi (ROS) için MAVLink düğümü (MAVROS) kullanılarak Pixhawk'dan uçuş bilgileri okunabilmektedir. Bu bilgileri okumak için Linux tabanlı Ubuntu 16.04 sürümü içinde ROS kullanılmaktadır.

4.2. Veri Kümesi

Çalışma boyunca arıza ve anormal durumların tespit edilmesi için çeşitli arıza senaryoları analiz edilmiştir. Bu çalışmada, güvenli uçuş günlüklerinden alınan Hava Laboratuvarı Arıza ve Anomali (ALFA) [28] veri seti kullanılmıştır.

ALFA veri seti, sabit kanatlı Carbon-ZT-28 model hava aracının ham uçuş günlüklerini içermektedir. Bu ham uçuş günlükleri yer istasyonundan İHA'ya müdahale edilerek oluşturulan yapay kontrol arızalarından elde edilmektedir. Sabit kanatlı hava araçlarının kontrol bileşenleri motor, kanatçık, dümen ve asansörden (aşağı yukarı hareketi sağlayan yapılar) oluşmaktadır. Bu kontrol bileşenlerinde oluşan arızaların izinsiz girişler sonucunda ortaya çıktığı kabul edilecektir.

ALFA veri serti gerçek kontrol bileşenleri ve gerçek arızalı test uçuş günlükleri içeren bir veri seti sağlamaktadır. Bu test uçuşları ABD'nin Pittsburgh havaalanlarında gerçekleştirilmiştir. Bu veri seti normal uçuş günlüklerinin yanı sıra farklı arızalara ait uçuş kayıtlarını sağlamaktadır. Veri seti güvenli uçuş verileri, kanatçık arızası, dümen arızası, motor arızası ve asansör arızası verilerinden oluşmaktadır. Bu verilerden sağlam uçuş verileri eğitim verisi olarak, geri kalan arıza verileri ise test verisi olarak kullanılacaktır.

4.2.1. Veri Formatı ve Arıza Türleri

ALFA veri setinde bulunan anormallikler ile 8 farklı ani kontrol yüzey arızası senaryosu oluşturulmuştur. Bu arızalar: Motorda oluşan tam güç kaybı, dümenin tam sol konumda sıkışması durumu, dümenin tam sağ konumda sıkışması durumu, asansörün yani yukarı aşağı hareketi sağlayan yapının sıfır (düz/hareketsiz) konumda takılı kalması durumu, sol kanatçığın sıfır konumunda takılı kalması durumu, sağ kanatçığın sıfır konumunda takılı kalması durumu, sağ ve sol kanatçıkların sıfır pozisyonunda takılı kalması durumu, dümen ve kanatçığın sıfır konumunda takılı kalması durumu senaryolarından oluşmaktadır.

Bu veri setinde toplamda 47 otonom uçuş için işlenmiş veriler bulunmaktadır. Bu uçuş verilerinin detayları Tablo 4.1'de verilmektedir [28,29].

Tablo 4.1. Uçuş verilerindeki hata türü, sayıları ve süreleri

Arıza Tipi	Test Uçuş Sayısı	Arızadan Önceki Uçuş Süreleri (saniye)	Arızalı Uçuş Süreleri (saniye)
Motor tam güç kaybı arızası	23	2.282	362
Dümenin sola sıkışma arızası	1	60	9
Dümenin sağa sıkışma arızası	2	107	32
Asansörün sıfır konumunda kalma arızası	2	181	23
Sol kanatçık sıfırda takılı kalma arızası	3	228	183
Sağ kanatçık sıfır konumunda kalma arızası	4	442	231
Sağ ve sol kanatçıkların sıfır konumunda kalma arızası	1	66	36
Dümen ve kanatçık sıfır konumunda kalma arızası	1	116	27
Güvenli uçuş	10	558	-
Toplam	**47**	**4.040**	**903**

4.2.2. ALFA Veri Setinden Özellik Çıkarımı

ALFA veri setindeki gerçek uçuş günlükleri çok sayıda parametre içermektedir. İHA bileşenlerine yönelik toplam arıza sayıları ve türleri Tablo 4.2'de gösterilmiştir.

Tablo 4.2. Arıza türleri ve sayıları

Sınıflar	Arıza Sayısı
Güvenli Uçuşlar (No Fault)	10
Motor (Engine) Arızası	23
Kanatçık (Aileron) Arızası	8
Dümen (Rudder) Arızası	4
Asansör (Elevator) Arızası	2
Toplam	47

ALFA veri setindeki günlük verilerinin içerisinden arıza ya da anormallik tespiti için gerekli olan özelliklerin çıkarılması gerekmektedir. Özellik seçiminde günlük verileri içerisinden çıkarılacak özellikler için bir özellik vektörü tasarlanması önerilmektedir. Bu özellikler: Sistem veya donanım özellikleri, IMU'dan alınan sensör verileri ve konum bilgisi verileri şeklinde kategorize edilmiştir. Özellik vektörü yapısı ve çalışmada kullanılmak üzere çıkarılan özellikler Tablo 4.3'te gösterilmektedir. Seçilen donanım veya sistem özellikleri, benzersiz olan özellikleri ortadan kaldırmayı amaçlamaktadır [12]. Seçilen donanım ve sistem özelliklerinin kullanılan hava

aracına özgü değil bütün hava araçlarında ortak olması beklenmektedir. Tek bir hava aracına özgü verilerin kullanılması durumunda, önerilen IGTS sadece döner kanat veya sadece sabit kanatlı İHA'lar için geçerli olacaktır. Ham uçuş günlükleri arasından seçilen özellikler hem sabit kanat hem de döner kanat İHA sistemlerinde kullanılmaktadır. Bu sayede önerilen İGTS modeli tüm İHA'lara uygulanabilir bir niteliğe sahip olmaktadır.

Tablo 4.3. Özellik vektörü bileşenleri

Kategori	Özellik Adı	Tanımı
Konum	Hız (x, y, z) (Velocity)	Sırasıyla x, y, z eksenlerinde ölçülen hızlar
IMU'dan Alınan Sensör Özellikleri	Açısal Hız (x, y, z) (Angular Velocity)	Sırasıyla x, y, z eksenlerindeki açısal hızlar
	Doğrusal İvme (x, y, z) (Linear Acceleration)	Sırasıyla x, y, z eksenlerinde doğrusal ivme
	Manyetik Alan (x, y, z) (Magnetic Field)	Sırasıyla x, y, z eksenlerinde manyetik alan değeri
	Akışkan Basıncı (Fluid Pressre)	Akışkan basıncı (sensörlerde kullanılan bir basınç değeri)
Sistem Özellikleri	Sıcaklık (Temperature)	Pil sıcaklığı
	Yükseklik (Rakım) Hatası (Altitude Error)	Geçerli yüksekliğin bir hata değeri
	Hava Hızı Hatası (Airspeed Error)	Mevcut hava hızının bir hata değeri
	İzlem Hatası (x) (Tracking Error(x))	X ekseninde izleme hatası
	WP Mesafesi (WP Distance)	İdeal konum ile mevcut konum arasındaki mesafe

4.3. Veri Ön İşleme

Bu bölümde, ALFA veri setinin analize hazırlanması amacıyla gerçekleştirilen veri ön işleme adımları açıklanmıştır. Veri ön işleme aşamaları, toplanan uçuş günlük bilgilerinin homojen bir yapıya sahip olması, eksik verilerin ele alınması ve analizde kullanılabilirliğin artırılması amacıyla gerçekleştirilmiştir.

ALFA veri seti, 47 farklı uçuşun uçuş günlük bilgilerini içeren bir veri setidir. Her bir uçuşun verileri ayrı bir Excel dosyasında saklanmıştır. Bu dosyaların her biri farklı sensörlerden alınan anlık verileri içermektedir.

Çalışmada kullanılacak özelliklerin seçimi, analizin odaklandığı alanı belirlemek adına büyük bir öneme sahiptir. Bu bağlamda, toplam 18 özellik parametresi belirlenmiştir. Veri seti içerisinde yer alan özellikler, farklı örnekleme frekanslarına sahip olmaları nedeniyle değişen boyutlara sahiptir. Bu boyut farklılıkları, veri analizinde bazı zorluklar doğurabilir. En yüksek boyut 3956 örnekleme, en düşük boyut ise 526 örneklemedir.

Farklı boyutlara sahip olan veri özelliklerinin homojen bir yapıya getirilmesi için interpolasyon işlemi uygulanmıştır. Bu adım, eksik verilerin tahmin edilmesi yoluyla veri boyutlarını eşitlemeyi amaçlamaktadır. Böylece, analizde kullanılacak özellik matrislerinin boyutları eşitlenmiştir. Interpolasyon sonucu elde edilen veriler, her özellik parametresi için aynı uzunluğa (1000 örneklem) sahip matrislere dönüştürülmüştür. Bu sayede, veri setinin homojenliği sağlanmış ve analiz sürekliliği sağlanmıştır. Elde edilen eşit uzunluktaki özellik matrisleri, analizdeki farklı özelliklerin birbirleriyle karşılaştırılabilir hale gelmesi amacıyla normalizasyon işlemine tabi tutulmuştur. Bu adım, verilerin belirli bir aralığa sıkıştırılarak istatistiksel analizin daha etkili bir şekilde gerçekleştirilmesine yardımcı olur.

Veri normalizasyonu için literatürde yaygın olarak kullanılan z-skor yöntemi tercih edilmiştir. Bu yöntem, her özellik sütununu örneklemler arasındaki ortalama ve standart sapma değerlerini kullanarak z-skora dönüştürür. Bu şekilde, verilerin dağılımı standartlaştırılarak analizdeki dengesizliklerin önüne geçilmiştir. Bu bölümde açıklanan veri ön işleme adımları, ALFA veri setinin analiz için uygun bir şekilde hazırlanması amacıyla gerçekleştirilmiştir. Bu adımlar, veri setinin homojenliğini ve kullanılabilirliğini artırmış, böylece daha güvenilir sonuçlar elde etme fırsatı sunmuştur.

4.3.1. İnterpolasyon

İnterpolasyon, eksik verilere veya sınırlı sayıdaki verilere dayalı olarak ara değerlerin tahmin edilmesi için kullanılan bir yöntemdir. Bu yöntem, mevcut veriler arasındaki ilişkiyi kullanarak eksik veya ara noktaların değerlerini tahmin etmeyi sağlamaktadır.

İnterpolasyon, matematiksel bir yaklaşım kullanarak bir fonksiyonun veya veri setinin düzenli bir şekilde geçtiği noktalar arasında kalan noktaların değerlerini hesaplamayı amaçlamaktadır. Bu süreç, veri setindeki eğilimleri ve düzenlilikleri analiz ederek, eksik veya ara noktaların değerlerini tahmin etmek için bir model veya fonksiyon oluşturmaktadır.

İnterpolasyon yöntemleri, veri setinin doğasına, düzenine ve istenen hassasiyete bağlı olarak değişebilmektedir. Yaygın interpolasyon yöntemleri arasında lineer interpolasyon, spline interpolasyon, pchip interpolasyon ve kübik interpolasyon bulunur. Bu yöntemler, verilerin düzgün bir şekilde takip edildiği veya veri setindeki eğilimlerin doğru bir şekilde yansıtıldığı durumlar için kullanılmaktadır.

İnterpolasyon, birçok alanda kullanılır, örneğin bilgisayar grafikleri, veri analizi, matematiksel modellerle çalışma, zaman serisi analizi ve mühendislik gibi alanlarda sıkça kullanılmaktadır. İnterpolasyon, eksik veya sınırlı veri setlerinde tahminler yapmak ve eksik bilgileri tamamlamak için önemli bir araçtır.

- **Doğrusal İnterpolasyon:** En basit interpolasyon yöntemlerinden biridir. İki bilinen nokta arasındaki doğruyu kullanarak eksik bir noktanın değerini tahmin etmektedir. Doğrusal

interpolasyon, iki nokta arasındaki doğruyu temsil eden bir denklem kullanmaktadır. Bu yöntem, doğrusal bir eğilim varsayımı yapmakta ve ara noktaları bu eğilime göre hesaplamaktadır. İki bilinen nokta arasındaki doğru denklemi, noktaların koordinatlarını kullanarak elde edilebilir. Doğrusal interpolasyon yöntemi, doğrusal eğilim gösteren veri setleri için uygundur. Ancak veri setindeki eğilim karmaşık veya eğrisel ise, doğrusal interpolasyon yetersiz veya hatalı sonuçlar verebilir. Bu durumda, daha karmaşık interpolasyon yöntemleri, örneğin doğrusal olmayan interpolasyonu veya kübik interpolasyon, daha iyi sonuçlar sağlayabilir.

- **Doğrusal Olmayan İnterpolasyon:** Polinomlar veya parçacık fonksiyonları kullanarak veri setindeki sıçramaları daha düzgün bir şekilde yakalamaktadır. Veri setindeki her noktanın etrafında bir eğri parçası oluşturulur. Doğrusal olmayan interpolasyon, veri setindeki sıçramaları ve ani değişimleri daha iyi yakalayabilir, böylece interpolasyon sonucunda daha doğru ve düzgün bir eğri elde edilebilmektedir. Ayrıca, bu interpolasyon yöntemi veri setindeki düzensizlikleri düzeltmek ve daha doğal bir şekilde veriyi temsil etmek için kullanılmaktadır. Doğrusal olmayan interpolasyonda, farklı düğüm noktaları arasında farklı polinom veya parçacık fonksiyonları kullanıldığından, veri setindeki her noktanın yakınında doğru bir şekilde uyan bir eğri elde edilebilmektedir. Bu, doğrusal olmayan interpolasyonu diğer interpolasyon yöntemlerinden ayıran önemli bir özelliktir. Bu interpolasyon yöntemi, grafiklerin oluşturulması, veri analizi ve eğri uydurma gibi birçok alanda yaygın olarak kullanılan bir interpolasyon yöntemidir.
- **Parçalı Kübik Hermite İnterpolasyon Polinomu (PCHIP):** Bu interpolasyon yöntemi veri noktaları arasında düzgün ve sürekli bir eğri oluşturmayı amaçlayan bir tür doğrusal olmayan interpolasyon yöntemidir. Bu yöntem, veri setindeki farklı örnekleme frekanslarına sahip özellikleri eşitlemek veya eksik verileri tahmin etmek amacıyla kullanılır. "Parçalı" terimi, eğrinin belirli bölgelerde farklı doğrusal olmayan polinomlar tarafından tanımlandığı anlamına gelir. PCHIP yöntemi, özellikle eğrinin kırılma noktalarında ve uç bölgelerinde düzgün geçiş sağlamak için tasarlanmıştır. Bu yöntem, veri setinin her noktasına ait eğri eğimleri (türevleri) kullanarak kırılma noktalarında eğriyi oluşturur. Bu sayede, veri noktaları arasında kesintisiz ve sürekli bir eğri elde edilir. PCHIP yöntemi, veri örnekleme frekanslarının farklı olduğu durumlar veya eksik veri noktalarının olduğu durumlar gibi karmaşık veri setlerinde başarılı sonuçlar verir. Bu yöntem, özellikle düşük seviyeli gürültü içeren veri setlerinde veri kaybını azaltmak ve eğriyi daha doğru bir şekilde yaklaştırmak için tercih edilir. Temel olarak, PCHIP yöntemi veri noktaları arasında sürekli ve pürüzsüz bir eğri oluşturarak, veri analizi, grafik tasarımı ve matematiksel modelleme gibi alanlarda kullanılan etkili bir interpolasyon yöntemidir.

- **Kübik İnterpolasyon:** Kübik eğri interpolasyonu, veri setindeki düzensizlikleri daha iyi ele almakta ve daha pürüzsüz bir interpolasyon sağlamaktadır. Her bir veri noktası için bir polinom parçası oluşturulmakta ve bu parçalar birleştirilerek tüm veri setini kapsayan bir eğri oluşturulmaktadır. Kübik interpolasyon, verilerin doğru bir şekilde yakalanmasını sağlamaktadır. Her bir polinom parçası, birinci, ikinci ve üçüncü dereceden terimler içerir ve bu nedenle "kübik" interpolasyon olarak adlandırılmaktadır. Kübik spline interpolasyonu, veri setindeki düzensizlikleri ve ani değişimleri daha iyi ele almaktadır. Her bir veri noktası arasında bir polinom parçası oluşturulmakta ve bu parçalar birleştirilerek tüm veri setini kapsayan bir eğri oluşturulmaktadır. Polinom parçalarının birleştirilmesi, eğri üzerinde süreklilik ve düzgünlük sağlamak için belirli kurallara göre gerçekleştirilmektedir. Kübik interpolasyon, veri noktalarının daha doğru bir şekilde yakalanmasını sağlamaktadır. Veri setindeki eğilimleri ve değişimleri pürüzsüz bir şekilde temsil etmek için kullanılmaktadır. Diğer interpolasyon yöntemlerine göre daha pürüzsüz bir interpolasyon elde etmek için tercih edilmektedir. Kübik eğri interpolasyonu, grafiklerin oluşturulması, veri analizi, animasyon ve eğri uydurma gibi birçok alanda yaygın olarak kullanılan bir interpolasyon yöntemidir. Veri setindeki düzensizlikleri daha iyi ele almak ve daha pürüzsüz bir eğri elde etmek önemli olduğunda tercih edilen bir yöntemdir. PCHIP yöntemi, kübik interpolasyonun bir alt kümesidir.

4.3.2. Veri Örnekleme ve İnterpolasyon İşlemi

Tez çalışmasında kullanılacak ALFA veri setinin yeniden örneklenmesi ve interpolasyon işlemi aşamaları aşağıdaki gibidir:

- Her biri farklı isimde kaydedilmiş Excel dosyaları (.mat) dosyasına dönüştürülmüştür.
- Deney verileri ayrı (.mat) dosyaları şeklinde bir klasörde depolanmıştır.
- **dir** işlevi ile klasördeki tüm (.mat) dosyalarının bir listesi alınmıştır.
- **resampledExperiments** adlı bir hücre dizisi oluşturularak örnekleme yapılan deneyler depolanmıştır.
- Oluşturulan Matlab kodu her bir dosyada döngüye girerek deneyleri örnekleme işlemine tabi tutmuştur.
- Deney değişkenleri **var1, var2, ..., var18** gibi isimlerle adlandırılmıştır.
- Yüklenen verilerden deney değişkenleri çıkarılıp **experimentVariables** hücre dizisinde saklanmıştır.
- Örnekleme için istenen ortak uzunluk 1000 olarak belirlenmiştir.
- Örnekleme faktörü, deneylerin orijinal uzunluğunun ortak uzunluğa bölünmesiyle elde edilmiştir.

- Her bir deney değişkeni için ayrı ayrı doğrusal **interpolasyon** kullanılarak örnekleme yapılmıştır.
- Örnekleme sonucu elde edilen değişkenler **resampledVariables** hücre dizisinde saklanmıştır.
- Örnekleme sonucu elde edilen değişkenler, orijinal dosya adının önüne "**resampled_**" öneki eklenerek yeni bir dosyaya kaydedilmiştir.
- Örnekleme dosya adları, **resampledExperiments** hücre dizisinde saklanmıştır.

4.3.3. Örnekleme Yapılmış verilerin Yüklenmesi ve Normalizasyon İşlemi

- Hazırlanan Matlab kodu örnekleme yapılmış deneylere ait klasördeki tüm (.mat) dosyalarının **dir** işlevi ile bir listesini alır.
- **loadedExperiments** adlı bir hücre dizisi oluşturularak yüklenen deneyler depolanır.
- Kod, her bir dosya için döngüye girerek örnekleme yapılmış deneyi **load** işlevi kullanarak geri yükler.
- Ortak uzunluk, ilk yüklenen deneyin boyutuna dayanarak belirlenir.
- Örnekleme yapılmış deney sayısı, özellik sayısı ve zaman bilgisi sütunu adı belirlenir.
- **normalizedFeatures** adlı yeni bir hücre dizisi oluşturulur ve normalize edilmiş özellikler saklanır.
- Kod, her bir deney ve her bir özellik için döngüye girer.
- Geçerli deneyden özelliği çıkarır.
- Zaman bilgisi sütununu alır.
- Z-skor normalizasyon yöntemiyle özelliği normalize eder.
- Normalize edilmiş özelliği matrise saklar.
- Tüm deneyler için normalize edilmiş özellikleri tek bir matrise birleştirir.

Bu sayede, veriler farklı boyutlarından bağımsız olarak aynı örnekleme boyutuna getirilmiş ve normalize edilmiş bir veri seti elde edilmiştir. Sonuç olarak, 10000x18 boyutunda normalize edilmiş bir eğitim veri kümesi ve 37000x18 boyutunda bir test veri kümesi elde edilmiştir.

4.3.4. Kullanılan Sınıflandırma Yöntemleri ve Parametreleri

Aşağıda Tez çalışmasında kullanılan tek sınıflı sınıflandırıcılar ve Matlab programında kullanılan fonksiyon isimleri verilmiştir. Her ne kadar bu yöntemlere ait daha fazla hiper parametre bulunsa da Tez çalışmasında varsayılan parametreler kullanılmış ve yüksek sınıflandırma performansı elde edilmiştir. Beklenen başarının elde edilemediği uygulamalarda bu parametreler optimize edilerek daha iyi sonuçlar elde edilebilir.

➢ **Tek Sınıflı Destek Vektör Makinesi (OC-SVM):**

- Kullanılan fonksiyon: **fitcsvm**
- Parametreler:
    - '**KemelFunction**': RBF (Radyal Tabanlı Fonksiyon)
    - 'Nu': 0.05 (Nu değeri, eğitim verisindeki anomalilerin oranını belirler)

➢ **Tek Sınıflı Rasgele Orman Sınıflandırıcısı (OC-RF):**

- Kullanılan Fonksiyon: **TreeBagger**
- Parametreler:
    - '**NumTrees**': 100 (Ağaç sayısı, ormanın büyüklüğünü belirler.)

➢ **Yerel Aykırı Faktör (LOF)**

- Kullanılan Fonksiyon: f**itlof**
- Parametreler:
    - '**NumNeighbors**': 20 (Komşu sayısı, bir noktanın lokal yoğunluğunu hesaplamak için kullanılır.)

➢ **Otomatik Kodlayıcı (Autoencoder):**

- Kullanılan Fonksiyonlar: **trainAutoencoder, predict**
- Parametreler:
    - Gizli katman boyutu: 10 (**input** boyutuna yakın bir değer seçilebilir.)
    - Aktivasyon fonksiyonu: **ReLu**
    - Optimizasyon algoritması: adam (gradyan tabanlı optimizasyon algoritması)
    - İterasyon sayısı sayısı: 1000

Her bir yöntem, verinin özelliklerini ve yapısını farklı şekillerde modellemek ve anormallikleri tespit etmek için kullanılan farklı yaklaşımlara sahiptir. OC-SVM, veriyi hiper düzlemle sınıflandırırken, OC-RF, bir sınıflandırma modeli olarak çalışılmaktadır. LOF lokal yoğunluk hesaplamalarına dayanırken, Autoencoder ise verinin özniteliklerini öğrenmeye dayalı bir yapıya sahiptir.

Bu yöntemler ve parametre değerleri veri boyutu ve özellikleri göz önünde bulundurularak seçilmiştir. Ancak her bir yöntemin performansı, veriye ve problem alanına bağlı olarak değişebilir.

Tez çalışmasında önerilen yenilik tabanlı – tek sınıflı sınıflandırma yönteminin en büyük avantajı eğitim verilerinin etiketsiz ve güvenli uçuşlardan oluşmasıdır. Bu sayede, saldırı tipi ne olursa olsun eğitilen model aykırı verileri rahatlıkla sınıflandırabilmekte ve izinsiz girişleri tespit edebilmektedir.

4.4. Yeniden Örnekleme Yöntemi

ALFA veri setinde sunulan verilerdeki her bir uçuş için başlangıç ve bitiş süreleri aynı olmasına rağmen örnekleme frekansı farklı olduğu için örnek sayısı da farklı olmaktadır. Bu nedenle veri setinin bu haliyle sınıflandırıcılara giriş olarak verilmesi mümkün olmamaktadır. Doğrusal interpolasyon ve yeniden örnekleme yapılarak her bir uçuş veri setinin örnek sayısı 1000 olarak düzenlenmiştir. Nihai veri setindeki uçuş sayıları ve toplam örnek sayıları Tablo 4.4'te gösterilmektedir.

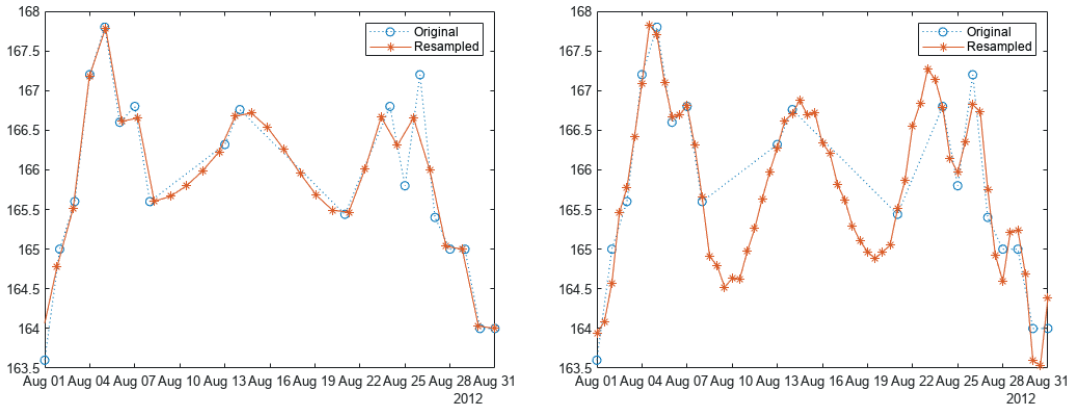
Tablo 4.4. Nihati veri setindeki uçuş ve örnek sayıları

Sınıflar	Uçuş Sayısı	Örnek Sayısı
Güvenli Uçuşlar (No Fault)	10	10 000
Motor (Engine) Arızası	23	23 000
Kanatçık (Aileron) Arızası	8	8 000
Dümen (Rudder) Arızası	4	4 000
Asansör (Elevator) Arızası	2	2 000
Toplam	47	47 000

Yeniden örnekleme yöntemi istatistik analizlerinde sıkça kullanılmaktadır. Bu yöntem mevcut veri kümesinden rastgele veriler alarak yeni veri setlerini oluşturmayı amaçlamaktadır. Her bir örnekleme seti üzerinden analiz yaparak istatistiksel sonuçlar elde edilmektedir. Orijinal bir veri kümesi (x) olsun, (n) gözlem ya da örneklem sayısı olduğu varsayılmıştır. Yeni oluşturulacak örneklem sayısı (b) olsun, (n) adet veriden rasgele veya istatistiksel sonuçlardan (b) tane seçilerek yeni veri seti oluşturulmaktadır. Bu duruma örnek olarak Şekil 4.3'te gösterilmektedir.

$$x = x_1, x_2, x_3, \dots, x_n \tag{4.1}$$

$$\forall x_i \ için\ i = 1, 2, \dots, b \tag{4.2}$$



Şekil 4.3. Yeniden örnekleme gösterimi

4.5. Performans Değerlendirme Metrikleri

Performans metrikleri makine öğrenmesi modellerinin veri setleri üzerindeki başarılarının nasıl ölçülebileceğini göstermektedir. Çoğu zaman bir problem üzerinde çalışırken elimizde birden fazla makine öğrenmesi modeli bulunmaktadır. Bu makine öğrenmesi yöntemleri arasından en başarılı ve en güvenilir yöntemin seçilmesi gerekmektedir. Bir diğer önemli nokta ise eğitim ve test kümelerindeki başarıları karşılaştırmaktır. Sadece genel doğruluk oranına bakmak çoğu zaman yeterli olmamaktadır. Örneğin %90 test başarımına sahip iki modelden hassasiyeti ya da duyarlılığı daha yüksek olan modelin belirlenmesi ve tercih edilmesi gerekir. Bu sayede eğitilen modelin eksiklikleri fark edilmekte ve bu problemlere özgü çözümler üretilmeye çalışılmaktadır. Tablo 4.5'de performans değerlendirme metriklerinin hesaplanmasında kullanılan istatistiksel parametreler görülmektedir. Bu tablo literatürde karşıtlık matrisi olarak bilinmektedir.

Tablo 4.5. Gerçek değerler ve tahmin edilen değerler arasındaki ilişki

		Doğru Sınıflar	
		Doğru	Yanlış
Tahmin Edilen Sınıflar	Doğru	Doğru Pozitif (DP)	Yanlış Pozitif (YP)
	Yanlış	Yanlış Negatif (YN)	Doğru Negatif (DN)

Tablo 4.5'te yer alan Doğru Pozitif (DP) sayısı, karşıtlık matrisinde doğru olarak sınıflandırılan ve gerçekte de doğru olan değerlerin sayısıdır. Yanlış Pozitif (YP) sayısı, doğru olarak sınıflandırılan fakat gerçekte yanlış olan değerlerin sayısıdır. Yanlış Negatif (YN), yanlış

olarak sınıflandırılan ve gerçekte de yanlış olan değerlerin sayısıdır. Doğru Negatif (DN) sayısı ise, yanlış olarak sınıflandırılan fakat gerçekte doğru olan değerleri göstermektedir [30] [31].

4.5.1. Hassasiyet (Precision)

Hassasiyet, bir sınıflandırma modelinin doğru olarak tahmin ettiği örneklerin gerçekten doğru olma oranını ölçmektedir. Yanlış pozitif oranını azaltmayı hedeflemektedir. Hassasiyet değeri 0 ile 1 arasında değişir, 1 en yüksek hassasiyeti temsil etmektedir. Hassasiyet metriği Denklem 4.3'deki gibi hesaplanmaktadır.

$$Hassasiyet\ (Precision) = \frac{DP}{DP + YP} \tag{4.3}$$

4.5.2. Duyarlılık (Recall)

Duyarlılık, gerçekte doğru olan örneklerin doğru bir şekilde sınıflandırılma oranını göstermektedir. Yanlış negatiflerin sayısını azaltmayı hedeflemektedir. Duyarlılık değeri 0 ile 1 arasında değişir, 1 en yüksek duyarlılığı temsil etmektedir. Duyarlılık metriği Denklem 4.4'deki gibi hesaplanmaktadır.

$$Duyarlılık\ (Recall) = \frac{DP}{DP + YN} \tag{4.4}$$

4.5.3. F1-Skoru (F1-Score)

F1-skoru, hassasiyet ve duyarlılık metriklerinin harmonik ortalamasını temsil etmektedir. Bu metrik kullanılan yöntemin ne derece doğru eğitildiğini, hassasiyet ve duyarlılık arasındaki dengeyi ölçmektedir. 0 ile 1 arasında değer almaktadır. F1-skoru metriği Denklem 4.5'deki gibi hesaplanmaktadır.

.

$$F1 - \text{Ölçüsü}\ (F1 - Score) = 2 * \frac{Hassasiyet * Duyarlılık}{Hassasiyet + Duyarlılık} \tag{4.5}$$

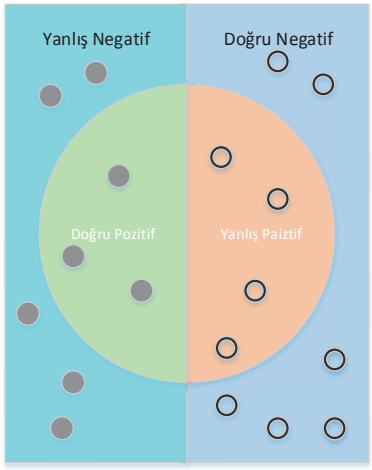
4.5.4. Doğruluk (Accuracy)

Doğruluk, sınıflandırma modelinin doğru olarak sınıflandırma oranını göstermektedir. Bu metrik, doğru tahminlerin toplam veri sayısına oranını hesaplamaktadır. Doğruluk değeri 0 ile 1

arasında değişir, 1 en yüksek doğruluğu temsil etmektedir. Doğruluk metriği Denklem 4.6'daki gibi hesaplanmaktadır.

$$Doğruluk\ (Accuracy) = \frac{DP + DN}{DP + DN + YP + YN} \tag{4.6}$$

Yukarıda verilen dört değerlendirme metriğinin şematik olarak gösterimi Şekil 4.4'te verilmiştir.



Şekil 4.4. Performans değerlendşrme matrisinin şematik gösterimi

5. YENİLİK TABANLI ANORMALLİK TESPİTİ

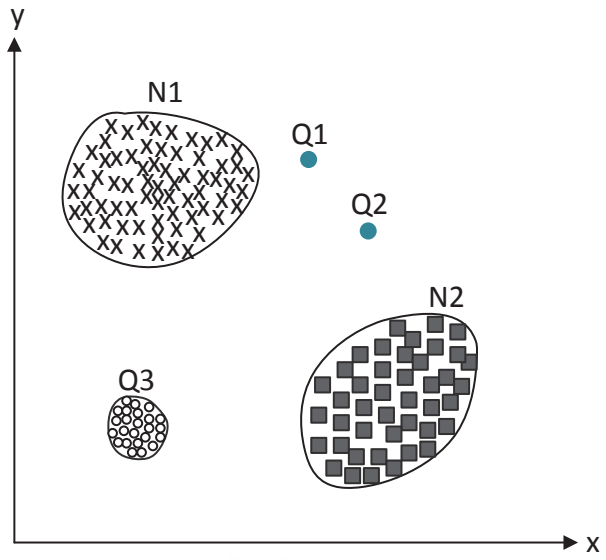
Günümüzde işletmeler, teknolojinin hızla ilerlemesi ve dijital dönüşüm sürecinin yaygınlaşmasıyla birlikte birçok avantaj elde etmiştir. Ancak bu gelişmelerle birlikte yeni riskler de ortaya çıkmıştır. Siber saldırılar, veri sızıntıları, sistem hataları, mali dolandırıcılıklar ve endüstriyel kazalar gibi anormal durumlar, işletmelerin karşılaşabileceği riskler arasında yer almaktadır. Bu riskler, işletmelerin finansal kayıplarına, itibar kaybına ve müşteri güveninin sarsılmasına yol açabilmektedir. Dolayısıyla, anormal durumları tespit etmek ve erken müdahalede bulunmak, işletmelerin başarısı ve sürekliliği açısından kritik bir öneme sahiptir. İşte bu noktada, anormallik tespit sistemleri devreye girmektedir.

Anormallik tespiti sistemleri, büyük veri kümeleri üzerinde analiz yaparak normal davranıştan sapmaları tespit eder ve potansiyel riskleri önceden belirleyerek sistemleri korumaktadır. Bu sistemler, gelişmiş veri analitiği, makine öğrenmesi ve yapay zekâ tekniklerini kullanarak anormal desenleri, davranışları veya olayları tespit etme yeteneğine sahiptir. Özellikle büyük veri setleri üzerinde çalışan bu sistemler, karmaşık yapılar arasında gizlenen anormallikleri tespit edebilmekte ve işletmelere değerli bir rekabet avantajı sağlayabilmektedir.

Anormallik tespit sistemleri, işletmelerin karşılaşabileceği çeşitli riskleri önceden belirleyen bir yaklaşım sistemi kullanmaktadır. Bu sistemler, verilerin sürekli olarak izlenmesi ve analiz edilmesi suretiyle anormal durumları hızlı bir şekilde tespit etmekte ve işletmeleri potansiyel zararlardan korumaktadır. Örneğin, bir ağ saldırısı durumunda, anormallik tespit sistemleri ağ trafiğini inceleyerek potansiyel saldırı işaretlerini belirleyebilmekte ve güvenlik önlemlerini hızla uygulayabilmektedir. Böylece, işletmeler siber saldırıların etkisini minimize edebilmekte ve sistematik bir şekilde korunabilmektedir.

Bunun yanı sıra, anormallik tespit sistemleri hataları ve mali dolandırıcılıkları tespit etme konusunda da oldukça etkili olmaktadır. İşletmeler, özellikle finansal kurumlar ve e-ticaret şirketleri, büyük miktarda finansal işlem verisine sahiptir. Bu verilerin analiz edilmesi ve anormal desenlerin tespit edilmesi, dolandırıcılık faaliyetlerini önlemek için kritik bir öneme sahiptir. Anormallik tespit sistemleri, finansal işlemleri ve kullanıcı davranışlarını inceleyerek, potansiyel dolandırıcılık işaretlerini belirler ve işletmelere hızlı bir şekilde uyarı göndermektedir. Böylece, müşteri hesaplarının güvenliği sağlanır, finansal kayıplar önlenebilir ve işletmenin itibarı korunabilmektedir.

Şekil 5.1'de iki boyutlu bir veri seti görülmektedir. Veri setindeki N1 ve N2 kümeleri normal verileri içermektedir. Ancak Q1, Q2 verisi ve Q3 kümesindeki veriler ise beklenmedik durumları yani anormal verileri temsil etmektedir.



Şekil 5.1. Normal ve aykırı veri kümeleri

5.1. Anormal Durumların ve Olayların Potansiyel Riskleri

İHA'lar son yıllarda birçok alanda kullanımı yaygınlaşan ve önemli avantajlar sunan teknolojik cihazlardır. İHA'lar, askeri operasyonlardan tarım sektörüne, taşımacılıktan hava fotoğrafçılığına kadar çeşitli alanlarda çeşitli avantajlar sunmaktadır. Bunlar arasında maliyet ve enerji verimliliği, erişim kolaylığı, çevresel etkilerin azalması ve zorlu veya tehlikeli ortamlarda görev yapma kabiliyeti sayılabilir. Ancak, İHA'ların artan kullanımıyla birlikte potansiyel riskler ve saldırılar da ortaya çıkmaktadır.

İHA'lara yapılan saldırılar hem güvenlik hem de gizlilik açısından önemli tehditler oluşturabilir. Bu saldırıların başlıca hedefleri arasında İHA'nın kontrolünün ele geçirilmesi, veri ve gizlilik ihlalleri, fiziksel zarar ve hatta terörist saldırılar yer almaktadır. Bu nedenle, İHA'lara yönelik saldırıları tanımlamak, anormal durumları belirlemek ve potansiyel riskleri değerlendirmek büyük önem taşır.

İHA'lara yönelik saldırıların potansiyel riskleri, çeşitli faktörlerden kaynaklanabilir. Öncelikle, İHA'ların kullanıldığı alanlarda saldırıları gerçekleştiren kişilerin amacı belirlenmelidir. Örneğin, askeri bir İHA'ya yönelik saldırılar, stratejik bilgilerin ele geçirilmesi veya misyonların engellenmesi gibi ciddi sonuçlar doğurabilmektedir. Benzer şekilde, ticari veya sivil alanda kullanılan İHA'lara yapılan saldırılar, veri hırsızlığı, sabotaj veya gizlilik ihlalleri gibi riskler oluşturabilmektedir.

İHA'lara yönelik saldırılar, farklı yöntemlerle gerçekleştirilebilmektedir. Saldırganlar, İHA'nın iletişim kanallarını hedef alabilir ve kontrol sinyallerini engelleyebilir veya bozabilmektedir. Böyle bir saldırıda, İHA'nın operatörü kontrolü kaybeder ve İHA kontrolsüz bir şekilde hareket edebilmekte veya düşürülebilmektedir. Ayrıca, saldırganlar, İHA'nın veri

bağlantısını ele geçirmeye veya manipüle etmeye çalışabilir, böylece İHA'nın gönderdiği verilerde değişiklikler yapabilmekte veya hassas bilgilere erişebilmektedir. Bu durum, hedeflenen İHA'nın görevlerini yerine getirememesine veya yanlış verilerle çalışmasına neden olabilmektedir.

İHA'lara yönelik saldırıları tanımlamak ve anormal durumları belirlemek için çeşitli yöntemler ve teknikler kullanılmaktadır. Örneğin, İHA'ların hareketlerini izlemek ve kontrol etmek için kullanılan algoritma ve yazılımlar, İHA'nın normal davranış kalıplarını belirleyebilmektedir. Bu şekilde, İHA'nın beklenmeyen bir şekilde sapma gösterdiği durumlar tespit edilebilmektedir. Ayrıca, İHA'nın iletişim sinyalleri ve frekans spektrumu analizi yaparak saldırıları tespit etmek mümkündür. Sinyal analizi, frekans engellemesi veya sinyal kesintileri gibi anormallikleri belirleyebilmektedir. İHA'nın kontrol sistemi ve sensör verilerini izlemek, beklenmeyen veri değerleri veya hareket desenleri gibi anormal durumları tespit etmek için etkili bir yöntemdir.

İHA'lara yönelik saldırılara karşı korunmak için çeşitli güvenlik önlemleri alınmalıdır. İlk olarak, İHA'nın iletişim kanallarının şifrelenmesi ve güvenliği sağlanmalıdır. İkincisi, İHA'ların kullanıldığı ağların güvenliği büyük önem taşımaktadır. Güvenlik açıklarının tespit edilmesi ve düzeltilmesi için sürekli bir ağ izleme ve güncelleme yapılmalıdır. Ayrıca, İHA'ların fiziksel erişimine dikkat edilmeli ve yetkisiz kişilerin İHA'ya müdahale etmeleri engellenmelidir.

Sonuç olarak, İHA'lara yönelik saldırılar potansiyel riskler taşımakta ve güvenlik açısından önemli tehditler oluşturabilmektedir. İHA'lara yapılan saldırıları tanımlamak, anormal durumları belirlemek ve potansiyel riskleri değerlendirmek, İHA teknolojisinin güvenli bir şekilde kullanılabilmesi için büyük önem taşımaktadır. Bu nedenle, İHA'ların güvenliği için gerekli önlemlerin alınması ve güvenlik sistemlerinin sürekli olarak güncellenmesi gerekmektedir. Yüksek düzeyde güvenlik sağlandığında, İHA'lar potansiyel faydalarını tam anlamıyla sunabilmekte ve güvenli bir şekilde kullanılabilmektedir.

İHA'lara yapılan saldırıları farklı şekillerde gerçekleşebilmekte ve çeşitli potansiyel riskler doğurabilmektedir. İHA'lara yönelik yaygın saldırı türlerinden bazıları şunlardır:

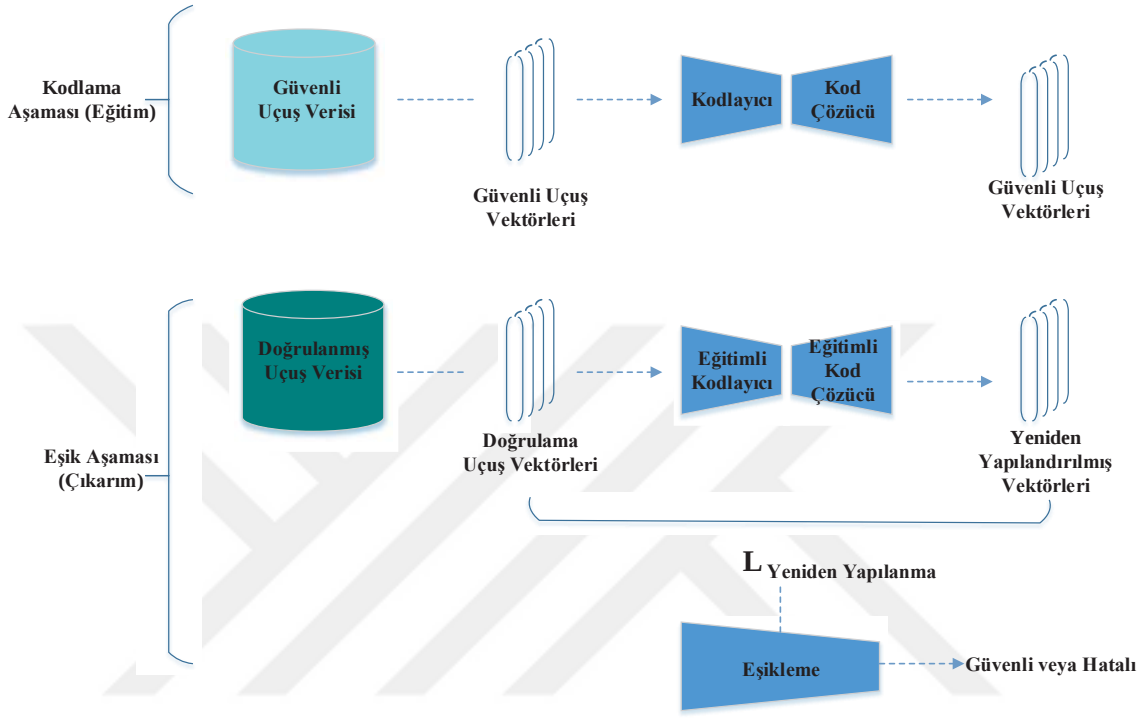
- Frekans engellemesi
- Sinyal izleme ve kaydetme
- Saldırı yazılımları ve zararlı kodlar

Bu saldırılar, İHA'lara yönelik potansiyel riskleri ortaya çıkarmaktadır. İHA'ların kontrolünün kaybedilmesi, veri ve gizlilik ihlalleri, maddi zararlar ve hatta can kayıpları gibi riskler söz konusu olabilmektedir. Bu nedenle, İHA'lara yapılan saldırıları tanımlamak ve anormal durumları belirlemek önem arz etmektedir.

İHA'lara yönelik saldırıları tespit etmek ve anormal durumları belirlemek için çeşitli yöntemler ve teknikler kullanılmaktadır. İHA'lara yönelik saldırıları tespit etmek için yaygın olarak kullanılan yöntemlerden bazıları şunlardır:

- Sayısal analiz

- Veri akışı izleme
- Davranışsal analiz
- Güvenlik duvarı ve kriptografi



Şekil 5.2. İHA saldırı tespit sisteminin çalışma mantığı

Şekil 5.2'de verilen arıza tespit modelinin genel yapısı şu şekildedir: İlk olarak, güvenli uçuş verileri uçuş günlüklerinden elde edilmektedir. Şekilde verilen model eğitim (kodlama) ve çıkarım (eşikleme) aşamalarından oluşmaktadır. Kodlama aşamasında, hatasız uçuş günlüklerinden elde edilen doğrulanmış özellik vektörleri eğitim için ele alınmaktadır. Bu vektör otomatik kodlayıcıya girdi olarak verilmektedir. Ardından, yeniden oluşturma kaybı elde edilmektedir. Eşikleme aşamasında ise, belirli bir eşik değeri ile karşılaştırma yapılarak yeniden oluşturma kaybı değerlendirilmektedir. Yapılan karşılaştırma sonucunda uçuş verilerinin güvenli ya da hatalı olduğu çıkarımı yapılmaktadır.

5.1.1. Frekans Engellemesi

Frekans engellemesi, İHA'lara yönelik gerçekleştirilen saldırılardan biridir ve ciddi potansiyel riskler taşımaktadır. Saldırganlar, İHA'nın kontrol frekansını engelleyerek iletişimin kesilmesini hedeflemektedirler. Bu saldırı türünde, saldırganlar İHA'nın kontrol sinyallerini ya da iletişim kanallarını bozarak normal iletişimi etkisiz hale getirmektedir.

Frekans engellemesi saldırısı, İHA'nın kontrolünün kaybedilmesine ve beklenmedik şekilde hareket etmesine yol açmaktadır. Örneğin, İHA'nın belirlenen alandan çıkması veya kontrolünün tamamen kaybedilerek başka bir yöne kontrolsüz bir şekilde ilerlemesi gibi durumlar ortaya çıkabilmektedir. Bu, hem İHA'nın kendisi için bir risk oluştururken hem de çevredeki insanlar ve mülkler için potansiyel tehlike yaratabilmektedir.

Frekans engellemesi saldırısının etkileri oldukça geniş kapsamlı olabilmektedir. İHA'nın kontrolünün kaybedilmesi, beklenmeyen hareketler yapması ve belirlenen güzergâhtan sapması, uçuş emniyetini tehlikeye atmaktadır. Özellikle yoğun insan bölgelerinde veya hassas bölgelerde gerçekleştirilen İHA uçuşlarında, bu durum ciddi sonuçlara yol açabilmektedir. İHA'nın kontrolünü ele geçiren saldırganlar, İHA'yı istedikleri şekilde kullanabilir veya yanlış amaçlarla kullanarak kişilere ve mülklere zarar verebilmektedir.

Ayrıca, frekans engellemesi saldırısı, İHA'nın veri bağlantısının kesilmesine ve bilgilerin kaybedilmesine de yol açabilmektedir. İHA'lar genellikle canlı video akışı veya diğer verileri gerçek zamanlı olarak aktarmaktadır. Saldırganların frekans engellemesiyle İHA'nın veri aktarımını engellemesi, İHA operatörlerinin sahadaki görüntüleri veya diğer önemli bilgileri kaybetmesine neden olmaktadır. Bu da İHA'nın etkinliğini ve kullanım amacını büyük ölçüde azaltmaktadır.

Frekans engellemesi saldırılarına karşı önlemler almak oldukça önemlidir. İlk olarak, İHA'ların kullanıldığı alanda frekans tarama ve izleme sistemi kullanılmaktadır. Bu sistemler, İHA'nın normal frekansından sapmasını tespit ederek saldırıyı erken tespit edebilmektedir. Ayrıca, İHA'ların frekanslarının şifrelenmesi veya gizli kanallar kullanılması da güvenliği artırmaktadır. Saldırı tespit ve koruma sistemleriyle donatılan İHA'lar, saldırıları algılayarak otomatik tepkiler verebilmekte veya operatörleri uyarabilmektedir.

Sonuç olarak, frekans engellemesi saldırıları İHA'lara yönelik ciddi bir risk oluşturmaktadır. İHA'ların kontrolünün kaybedilmesi ve iletişimlerinin kesilmesi, beklenmeyen hareketler ve güvenlik açıklarına yol açabilmekte bu nedenle, İHA kullanıcılarının frekans engellemesi, saldırılarına karşı önlemler alması ve güvenlik sistemlerini etkin bir şekilde kullanabilmesi gerekmektedir. Bu sayede, İHA'ların güvenli ve başarılı bir şekilde kullanılması sağlanabilmektedir.

5.1.2. Sinyal İzleme ve Kaydetme

Sinyal İzleme ve Kaydetme, İHA'lara yönelik yapılan saldırı türlerinden biri olmakta ve ciddi potansiyel riskler taşımaktadır. Saldırganlar, İHA'nın iletişim sinyallerini izleyerek ve kaydederek İHA'nın faaliyetlerini takip edebilmektedirler. Bu saldırı türü, özellikle askeri veya güvenlik odaklı operasyonlarda büyük bir endişe kaynağıdır çünkü saldırganlar bu şekilde stratejik bilgilere erişme potansiyeline sahip olmaktadırlar.

Sinyal izleme ve kaydetme saldırılarının ana hedefi, İHA'nın iletişim sinyallerini ele geçirmek ve analiz edebilmektir. İHA'lar genellikle bir kontrol merkezi veya operatör aracılığıyla kontrol edilmekte ve iletişim kanalları üzerinden bilgi alışverişi yapmaktadır. Saldırganlar, İHA'nın iletişim kanallarını izleyerek, İHA'nın konumunu, hızını, rotasını ve diğer önemli verileri belirleyebilmektedirler. Bu bilgileri kullanarak, İHA'nın mevcut ve gelecekteki hareketlerini tahmin etmek mümkün olabilmektedir.

Bu tür saldırılar, hassas verilere erişimi de beraberinde getirebilmektedir. İHA'lar, genellikle gözetim, keşif veya istihbarat toplama amaçlarıyla kullanılmaktadır. İletişim kanallarının izlenmesi ve kaydedilmesi, İHA üzerinden aktarılan görüntüler, haritalar, coğrafi bilgiler ve diğer hassas verilerin ele geçirilmesine yol açabilmektedir. Bu durum, ulusal güvenlik açısından ciddi bir tehdit oluşturabilir ve saldırganlara stratejik bilgilerin ortaya çıkması veya saldırı planlarının ifşa edilmesi gibi büyük avantajlar sağlayabilmektedir.

Sinyal izleme ve kaydetme saldırılarına karşı alınabilecek önlemler bulunmaktadır. İlk olarak, İHA'ların iletişim kanallarının güvenliği sağlanmalı ve şifreleme teknikleri kullanılmalıdır. İletişim sinyallerinin şifrelenmesi, saldırganların sinyali anlamalarını veya izlemelerini zorlaştırmaktadır. Ayrıca, sinyal karıştırma veya gürültü ekleme gibi teknikler de kullanılabilir, böylece sinyal izleme girişimleri engellemektedir.

Operasyonların gizliliği de büyük önem taşımaktadır. İHA'nın faaliyetleri ve kullanılacağı bölgelerin gizli tutulması, saldırganların hedef belirlemesini ve saldırı planlarını hazırlamasını operasyon gizliliği acısından önem taşımaktadır. Aynı zamanda, İHA'ların güvenlik sistemleri düzenli olarak güncellenmeli ve güvenlik açıkları kapatılmalıdır. Saldırılara karşı güvenlik yazılımları ve ağ filtreleme çözümleri kullanmak gerekmektedir.

Sonuç olarak, sinyal izleme ve kaydetme saldırıları, İHA'lara yönelik önemli bir tehdit oluşturmaktadır. Bu saldırılar, İHA'nın hareketlerini tahmin etme, hassas verilere erişme ve stratejik bilgilerin ele geçirilmesi gibi potansiyel riskler taşımaktadır. İHA kullanıcıları ve operatörleri, güvenlik önlemlerini eksiksiz bir şekilde uygulamalı ve sinyal izleme saldırılarına karşı etkin bir savunma sağlamalıdır. Böylece, İHA'ların güvenliği ve verimliliği sağlanabilir, ulusal güvenlik tehditleri minimize edilebilmekte ve İHA teknolojisinin avantajlarından tam olarak yararlanılmaktadır.

5.1.3. Saldırı Yazılımları ve Zararlı Kodlar

Saldırı Yazılımları ve Zararlı Kodlar, İHA'lara yönelik ciddi bir tehdit oluşturan saldırı türlerindendir. Saldırganlar, İHA'nın kontrol sistemine zararlı yazılımlar veya kodlar enjekte ederek İHA'yı ele geçirmeye veya kontrol etmeye çalışırlar. Bu tür saldırılar, İHA'nın beklenmeyen hareketler yapmasına ve kontrolünün tamamen kaybedilmesine yol açmaktadır. Bu da ciddi

potansiyel riskler doğurur ve hem güvenlik hem de operasyonel açıdan büyük sorunlar yaratabilmektedir.

Saldırı yazılımları ve zararlı kodlar, İHA'nın işletim sistemlerine, yazılımlarına veya kontrol altyapısına zarar vermek için kullanılmaktadır. Saldırganlar, İHA'nın işlevlerini bozacak veya manipüle edecek yazılımları enjekte edebilmektedirler. Bu şekilde, İHA'nın programlanmış görevleri yerine getirmemesi veya saldırganın istediği şekilde yönlendirilmesi gibi durumlar ortaya çıkmaktadır.

Örneğin, saldırı yazılımları ve zararlı kodlar aracılığıyla İHA'nın kontrol sistemine sızılabilmekte ve saldırganlara İHA'nın tam kontrolünü sağlamaktadır. Bu durumda, saldırgan İHA'yı istediği gibi yönlendirebilir, programlanmış görevlerini yerine getirmesini engelleyebilir veya İHA'yı tamamen devre dışı bırakmaktadır. İHA'nın beklenmeyen hareketleri veya kontrolünün kaybedilmesi, hem uçuş güvenliği hem de çevredeki insanların güvenliği için büyük bir risk oluşturmaktadır.

Bu tür saldırılara karşı önlemler almak büyük önem taşımaktadır. İlk olarak, İHA'ların yazılım güvenliği ve güncelliği sağlanmalıdır. İHA üreticileri ve kullanıcıları, yazılım güvenlik açıklarını sürekli olarak izlemeli ve güvenlik yamalarını zamanında uygulamalıdır. Ayrıca, güvenli ve şifrelenmiş iletişim protokolleri kullanılmalıdır. İHA iletişim kanalları, güvenlik açıklarına karşı korunmalı ve saldırılara karşı dirençli olacak şekilde tasarlanmalıdır.

Bunun yanı sıra, güvenlik duvarları, anti virüs yazılımları ve zararlı yazılım tespit sistemleri gibi güvenlik çözümleri kullanılmalıdır. Bu çözümler, saldırı yazılımlarını ve zararlı kodları tespit etmek ve engellemek için aktif olarak çalışmaktadır. Ayrıca, güvenlik açıkları veya saldırı girişimleri tespit edildiğinde, sistemleri korumak için hızlı tepki ve müdahale mekanizmaları da gerekmektedir.

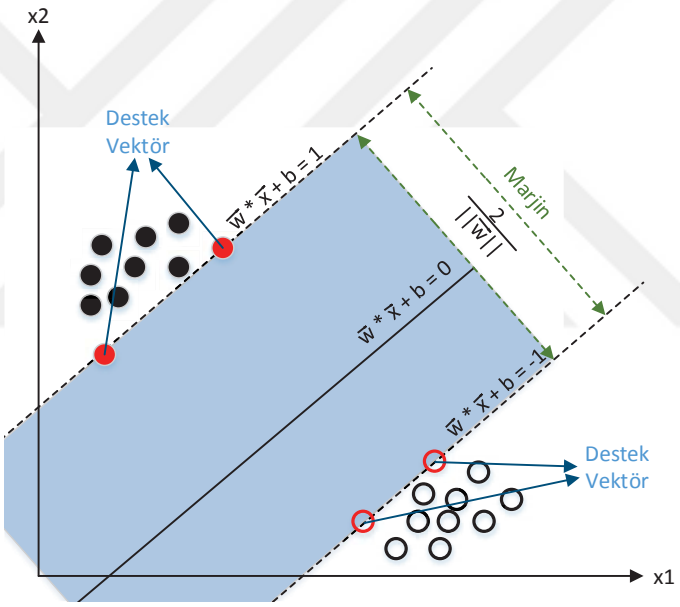
Sonuç olarak, saldırı yazılımları ve zararlı kodlar İHA'ların güvenliğini ve işlevselliğini ciddi şekilde etkileyebilmektedir. İHA üreticileri, kullanıcıları ve güvenlik uzmanları, sürekli olarak güvenlik önlemlerini gözden geçirmeli, güncel tehditlere karşı savunma mekanizmalarını güçlendirmeli ve saldırılara karşı etkin bir şekilde korunma sağlamalıdır. Yüksek güvenlik standartlarına sahip İHA'lar, siber saldırılara karşı daha dirençli olacak ve güvenlik açıkları minimize edilecektir. Bu da İHA teknolojisinin güvenli ve verimli bir şekilde kullanılmasını sağlayacak ve İHA'ların potansiyel risklerini azaltacaktır.

5.2. Destek Vektör Makinesi (SVM)

Destek Vektör Makinesi (SVM), makine öğrenmesi alanında sınıflandırma ve regresyon problemlerini çözmek için kullanılan bir algoritmadır. SVM, veri noktalarını daha iyi sınıflandırmak veya tahmin etmek için matematiksel olarak optimize edilmiş bir hiper düzlem oluşturmaktadır.

SVM'nin çalışma prensibi, veri noktalarını uzayda ayıran bir hiper düzlemi bulmaktır. Bu hiper düzlem, sınıflar arasında mümkün olan en büyük marjin elde etmek için optimize edilmektedir. Marj, hiper düzlemle en yakın veri noktaları arasındaki mesafeyi ifade etmektedir. SVM, bu marjin maksimize etmek için destek vektörler olarak adlandırılan veri noktalarını kullanmaktadır. Destek vektörler, hiper düzleme en yakın olan ve karar sınırının belirlenmesinde önemli olan veri noktalarıdır.

Sınıflandırma problemlerinde, SVM, veri noktalarını iki farklı sınıfa ayırmak için kullanılmaktadır. Örneğin, veri noktalarının iki farklı sınıfa ait olduğu bir örnekte, SVM bir sınıfın veri noktalarını bir tarafında, diğer sınıfın veri noktalarını ise diğer tarafında ayıracak bir hiper düzlem oluşturur. Böylece, yeni gelen bir veri noktasının hangi sınıfa ait olduğunu tahmin etmek için bu hiper düzlem kullanabilir. Şekil 5.3'te SVM yönteminin genel yapısı gösterilmektedir.



Şekil 5.3. SVM sınıflandırıcısının şematik gösterimi

SVM genellikle sınıflandırma problemlerinde kullanılan gözetlemeli öğrenme yöntemleri arasında yer almaktadır. Bir düzlem üzerinde yerleştirilmiş noktaları ayırmak için bir hiper düzlem doğrusu çizilmektedir. Bu doğrunun, iki sınıf noktaları için maksimum uzaklıkta olması amaçlanmaktadır.

Şekil 5.3'te siyah ve beyaz olmak üzere iki farklı sınıf bulunmaktadır. Sınıflandırma problemindeki asıl amaç gelecek verinin hangi sınıfta yer alacağına karar vermektir. Bu sınıflandırmayı yapmak için iki sınıfa ayıran bir hiper düzlem çizgisi çekilmekte ve bu çizgi +1 veya -1 arasında kalan bölgeye marjin adı verilmektedir. Marjin ne kadar geniş ise iki veya daha fazla sınıf o kadar iyi ayrışmaktadır.

$$f(x) = \begin{cases} 0, w^T * x + b < 0, \\ 1, w^T * x + b \geq 0 \end{cases} \quad (5.1)$$

Denklem 5.1'de **w**; ağırlık vektörü, **x**; girdi vektörü, **b**; sapmadır. Yeni bir değer için çıkan sonuç 0'dan küçükse, beyaz noktalara daha yakın olacaktır. Tam tersi, çıkan sonuç 0'a eşit veya büyükse, bu durumda siyah noktalara daha yakın olacaktır [32].

Regresyon problemlerinde, SVM, veriler arasındaki ilişkiyi analiz etmek için kullanılmaktadır. SVM regresyonunda, hedef değerler birbirinden farklı sınıflara ayrılmamaktadır. Hiper düzlem, veri noktalarının mümkün olan en iyi şekilde dağılmasını sağlamakta ve yeni gelen veri noktalarının hedef değerlerini tahmin etmek için kullanılabilmektedir.

SVM, özellikle doğrusal olarak ayrılabilir veri noktaları için etkilidir. Ancak, çoğu gerçek dünya probleminde veri noktaları doğrusal olarak ayrılamamaktadır. Bu durumda, SVM'nin yapısında doğrusal olmayan çekirdek fonksiyonları kullanılmaktadır. Çekirdek yöntemleri, verileri daha yüksek boyutlu bir uzaya taşımakta ve bu uzayda lineer olarak ayrılabilir hale gelmektedir.

SVM, sınıflandırma ve regresyon problemlerinde etkili sonuçlar veren bir algoritmadır. Özellikle veri noktaları arasında net bir ayrımın olmadığı karmaşık problemlerde başarılı olmaktadır. SVM'nin avantajları arasında yüksek boyutlu verilerle iyi çalışma, az miktarda destek vektör kullanması ve çekirdek yöntemleriyle esneklik sağlanmasıdır. Ancak, büyük veri kümeleriyle çalışırken hesaplama maliyeti yüksek olabilmektedir.

5.3. Tek Sınıflı Destek Vektör Makinesi (OC-SVM) ile Anormallik Tespiti

İHA'ların kullanımının hızla artmasıyla birlikte, İHA'lar hedef haline gelerek, saldırı tehditlerine maruz kalma potansiyelleri de artmıştır. Bu nedenle, İHA'lara karşı etkili koruma önlemleri almak ve saldırıları tespit etmek, güvenli bir İHA kullanımının sağlanması açısından büyük önem taşımaktadır. Tez çalışmasında İHA'lara yapılan saldırıları tespit etmek için kullanılan yöntemlerden biri tek sınıflı destek vektör makinesi (OC-SVM) yöntemidir.

OC-SVM, temel olarak normal davranışları temsil eden verilere dayalı bir model oluşturmaktadır. Eğitim aşamasında, OC-SVM, sadece güvenli uçuşlara ait veri kümesini kullanarak bir hiper düzlem oluşturmaktadır. Test aşamasında, İHA'nın gerçek zamanlı sensör verileri veya geçmiş verileri kullanılarak, oluşturulan hiper düzlemin dışında kalan veriler tespit edilmektedir. Bu veriler anormal olarak sınıflandırılmakta ve bir saldırı durumu olduğu kabul edilmektedir.

OC-SVM, İHA saldırı tespiti için etkili bir yöntemdir, ancak her uygulama ve senaryoda farklı parametreler gerektirebilmektedir. Veri kümesinin özelliklerine, saldırıların çeşitliliğine ve diğer faktörlere bağlı olarak OC-SVM parametreleri ayarlanmalıdır.

Sonuç olarak, İHA'lar günümüzde birçok farklı alanda kullanılmaktadır ve bu kullanım potansiyel saldırı tehditlerini de beraberinde getirmektedir. İHA'lara yapılan saldırıları tespit etmek için OC-SVM gibi yöntemlerin kullanılması, İHA güvenliğinin sağlanması ve saldırılara karşı etkili önlemler alınması açısından önemlidir. OC-SVM, İHA'ların normal davranışlarını temsil eden verileri kullanarak anormal davranışları tespit etmek için bir araç olarak kullanılabilmektedir. Ancak, bu yöntemlerin etkinliği ve güvenilirliği için sürekli araştırma ve geliştirme çalışmalarının yapılması gerekmektedir.

Matematiksel model yapısında OC-SVM yöntemi, SVM de olduğu gibi veri kümelerini doğrusal olarak bir veya birden fazla sınıfa bölmek yerine, sadece etiketsiz güvenli uçuş verilerine yoğunlaşmaktadır. Veri noktalarını çekirdek işlevi tarafından belirlenen çekirdek uzayına eşleyerek orijinden maksimum marjinle ayırmaktadır [33][34]. Denklem 5.2 orijin ile eşleşen noktalar arasındaki mesafeyi ayırıcı bir hiper düzlem için ikinci dereceden bir optimizasyon problemi önermektedir.

$$\min \frac{1}{2}\left|\left|w\right|\right|^2 - vnp + \sum_{i=1}^{n} \varepsilon_i \tag{5.2}$$

$$\begin{aligned} & s.t\langle w, \varphi(x_i)\rangle \geq p - \varepsilon_i, \\ & \varepsilon_i \geq 0, \qquad i = 1, 2, \ldots, n \end{aligned} \tag{5.3}$$

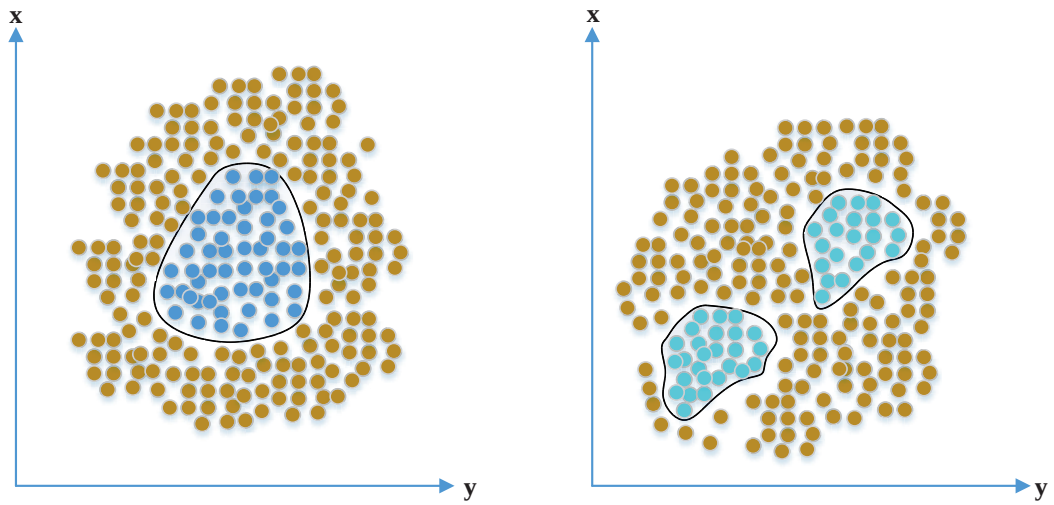
Denklem 5.3'te φ, çekirdek işlevini tanımlayan değerdir, ε_i, değişken değer, $v \in [0, 1]$, uzak noktaların oranını temsil eden bir sabit değer, p, verilen bir noktanın tahmini yoğunluğunun bölgeye ait olup olmadığını belirleyen karar değeridir.

$$h(x) = sign(w^{*T}\varphi(x) - p^*) \tag{5.4}$$

Karar fonksiyonu $h(x)$, Denklem 5.4'te gösterilmiştir.

$$\begin{aligned} max_a \; & -\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} a_i a_j K(x_i, x_j) \\ & s.t \;\; \sum_{i=1}^{n} a_{i=vn,} \\ & 0 \leq a_i \leq 1, \;\; i=1,2\ldots,n \end{aligned} \tag{5.5}$$

Denklem 5.5'te problem çözümünde $i > 0$'i sağlayan x_i noktalarına destek vektörleri denmektedir [33][34].



Şekil 5.4. OC-SVM'nin şematik gösterimi

Şekil 5.4'te OC-SVM'nin şematik yapısı gösterilmektedir. Şekildeki açık ve koyu mavi semboller normal davranışları, turuncu semboller ise anormal davranışları temsil etmektedir. OC-SVM ile İHA'larda anormallik tespiti için aşağıdaki adımlar izlenmektedir.

Veri Toplama: İlk adım, İHA'ların normal davranışlarını temsil eden bir veri kümesi toplamaktır. Bu veri kümesi, İHA'ların normal uçuş hareketlerini, sensör verilerini ve diğer ilgili bilgileri içermelidir. Bu bilgiler Bölüm 4.3.2'de detaylı olarak verilmiştir. Örneğin, İHA'nın irtifası, hızı, rotasyon açıları gibi öznitelikler bu veri kümesinde yer almaktadır.

Veri Önişleme: Veri kümesi toplandıktan sonra, veri önişleme adımları uygulanmıştır. Bu aşamada, öznitelikleri normalize etmek, eksik verileri tamamlamak ve veri boyutlarını eşitlemek gibi işlemler gerçekleştirilmiştir.

OC-SVM'nin Eğitimi: Veri kümesi önişleme adımlarından geçtikten sonra, OC-SVM algoritması kullanılarak bir sınıflandırma modeli oluşturulur. OC-SVM, normal davranışları (güvenli uçuşlar) temsil eden verileri kullanarak, bir hiper düzlem oluşturmaktadır. Bu hiper düzlem, normalden sapma gösteren verileri aykırı veri olarak sınıflandırmaktadır. OC-SVM eğitimi, uygun hiper parametrelerin seçimi ve modelin optimizasyonunu içermektedir.

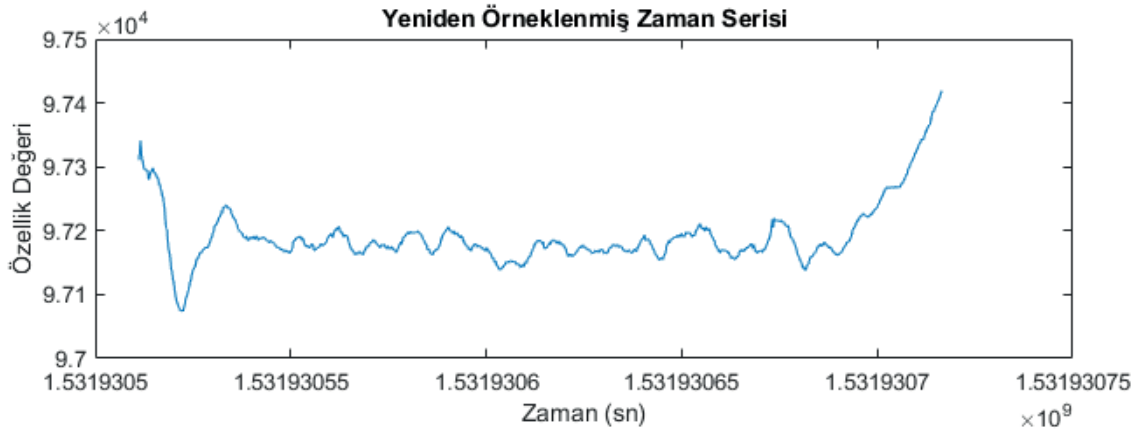
Saldırı Tespiti: Eğitilen OC-SVM modeli, yeni gelen veriler üzerinde test edilmektedir. Bu adımda, İHA'nın gerçek zamanlı sensör verileri veya geçmiş verileri modelleme için kullanılmaktadır. Test verileri, oluşturulan hiper düzlem tarafından kabul edilen bir marjın dışında kalıyorsa, bu veriler anormal olarak sınıflandırılmakta ve bir saldırı durumu olduğu düşünülmektedir. Anormal durumlar motor, kanatçık, dümen ve asansör arızalarını içermektedir.

Performans Değerlendirmesi: Bu aşamada, doğruluk, kesinlik, hassasiyet ve F1-sıkor gibi metrikler kullanılmaktadır. Ayrıca, yanlış pozitif ve yanlış negatif oranları gözlemleyerek sistem hatalarını analiz etmek mümkündür. Performans değerlendirmesi, sistemin güvenilirliğini ve

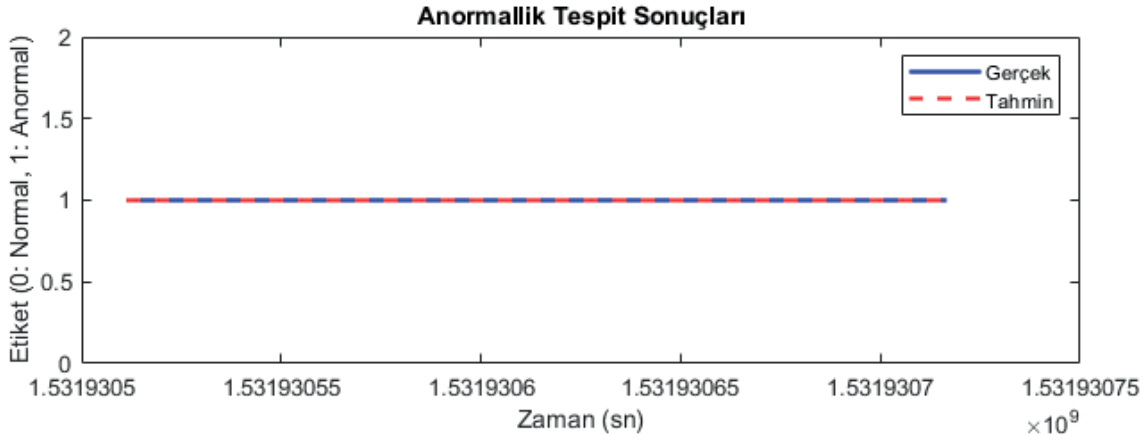
etkinliğini belirlemek için önemli bir adımdır. Performans metrikleri bütün arıza modelleri için hesaplanmıştır.

5.3.1. OC-SVM ile Motor Arızalarının Tespiti

OC-SVM'nin motor arızasına ait yeniden örneklenmiş verilerle yapılan test işleminin başarı oranı %100 olarak elde edilmiştir. Şekil 5.5'te, yeniden örneklenmiş, motor arızasına ait bir zaman serisi görülmektedir. Şekildeki grafiğin x-ekseni zamanı, y-ekseni ise özellik değerini temsil etmektedir. Motor arızası anomali tespitinde kullanılan 23.000 adet arızalı verinin tamamı doğru olarak sınıflandırılmıştır. Şekil 5.6'da gerçek ve tahmin edilen arıza tipi gösterilmektedir.



Şekil 5.5. Yeniden örneklenmiş motor arızası zaman serisi



Şekil 5.6. Motor arızasına ait gerçek ve tahmin edilen OC-SVM sonuçları

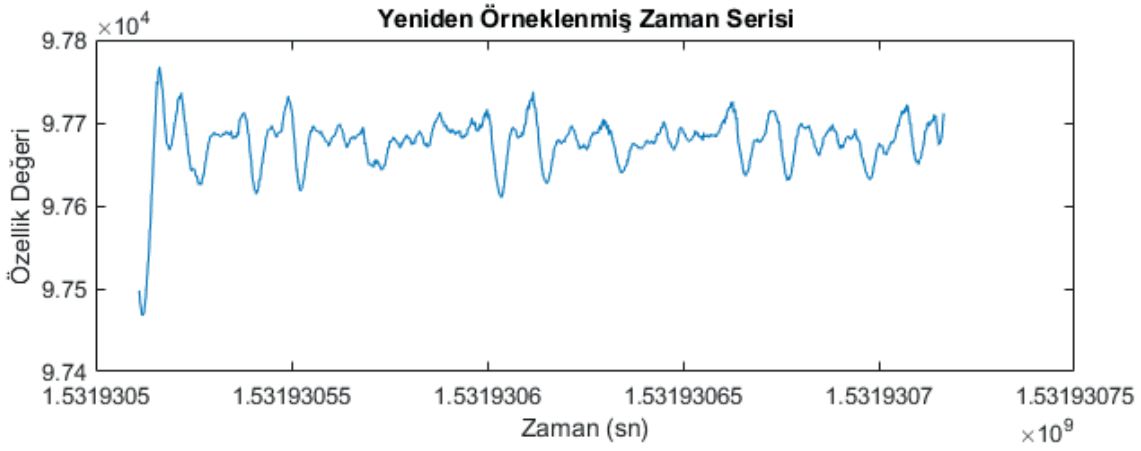
Motor arızası tespitinde kullanılan performans metrikleri Tablo 5.1'de görülmektedir.

Tablo 5.1. Motor arızası için OC-SVM performans değerlendirmesi

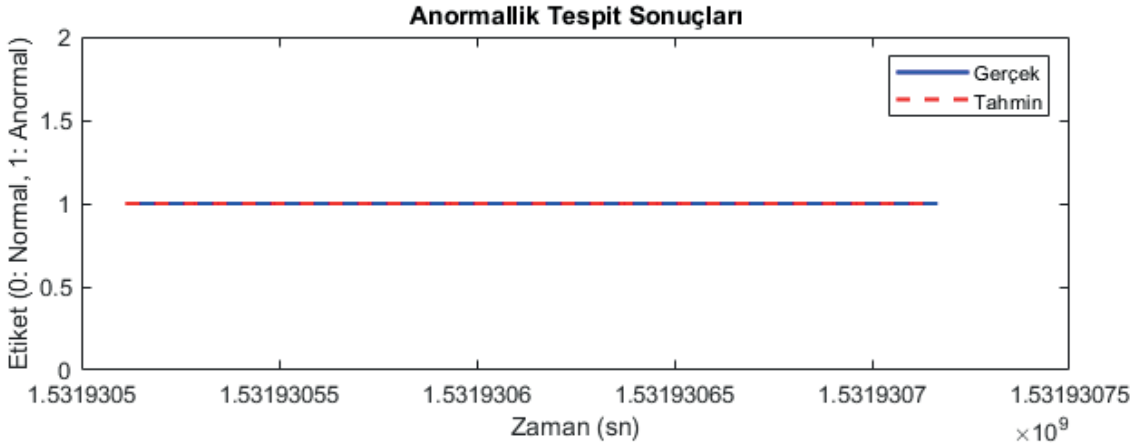
Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

5.3.2. OC-SVM ile Kanatçık Arızalarının Tespiti

Bu çalışmada, kanatçık arızasına ait uçuş günlükleri verileri kullanılarak OC-SVM modeli eğitilmiştir. Eğitim sonrasında, 8000 adet örnek veri ve 18 özellik parametresi ile kanatçık arızalarının tespit edilmesi için test işlemi gerçekleştirilmiştir. Elde edilen sonuçlar dikkate alındığında, modelin test verisi üzerinde %100 başarı elde ettiği görülmüştür. Şekil 5.7'de ve Şekil 5.8'de sırasıyla yeniden örneklenmiş test veri setindeki özellik zaman serisi ve test sonuçları görülmektedir.



Şekil 5.7. Yeniden örneklenmiş kanatçık arızası zaman serisi



Şekil 5.8. Kanatçık arızasına ait gerçek ve tahmin edilen OC-SVM sonuçları.

Hassasiyet, duyarlılık, F1-Skoru ve doğruluk ölçütleri değerlendirildiğinde, tüm ölçütlerin 1 olarak hesaplandığı gözlemlenmiştir. Bu durum, OC-SVM modelinin test verilerindeki kanatçık arızası örneklerini doğru ve eksiksiz bir şekilde sınıflandırdığını göstermektedir. Yani, modelin tespit ettiği herhangi bir kanatçık arızası örneği, gerçek arıza örneği olarak kesin bir şekilde doğrulanmıştır.

Bu sonuçlar, eğitilmiş OC-SVM modelinin kanatçık arızasına ait uçuş günlükleri verilerini etkili bir şekilde sınıflandırdığını ve test aşamasında mükemmel bir başarı elde ettiğini göstermektedir. Bu başarılı sonuçlar, modelin uygulamada potansiyel bir arıza tespit yöntemi olarak değerlendirilebileceğini göstermektedir. Kanatçık arızası için yapılan performans değerlendirmesi Tablo 5.2'de gösterilmektedir.

Tablo 5.2. Kanatçık arızası için OC-SVM performans değerlendirmesi

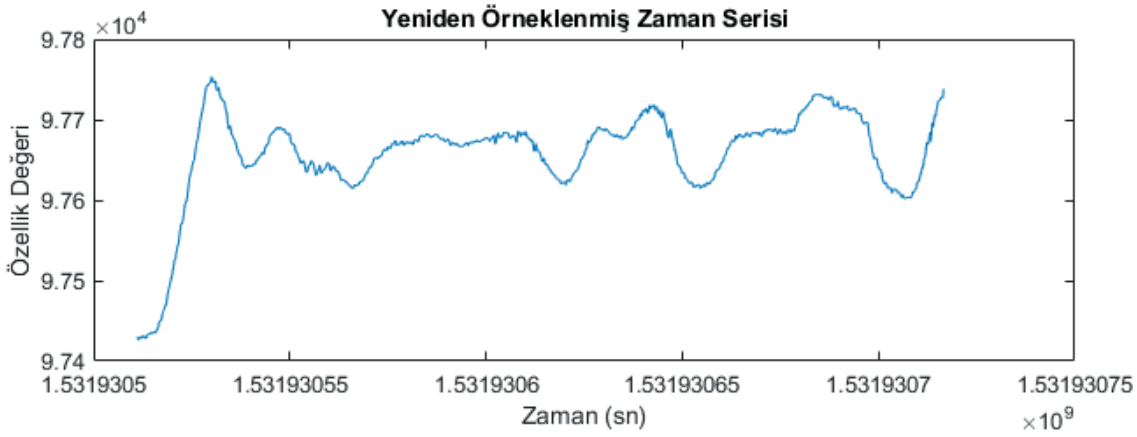
Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

5.3.3. OC-SVM ile Dümen Arızalarının Tespiti

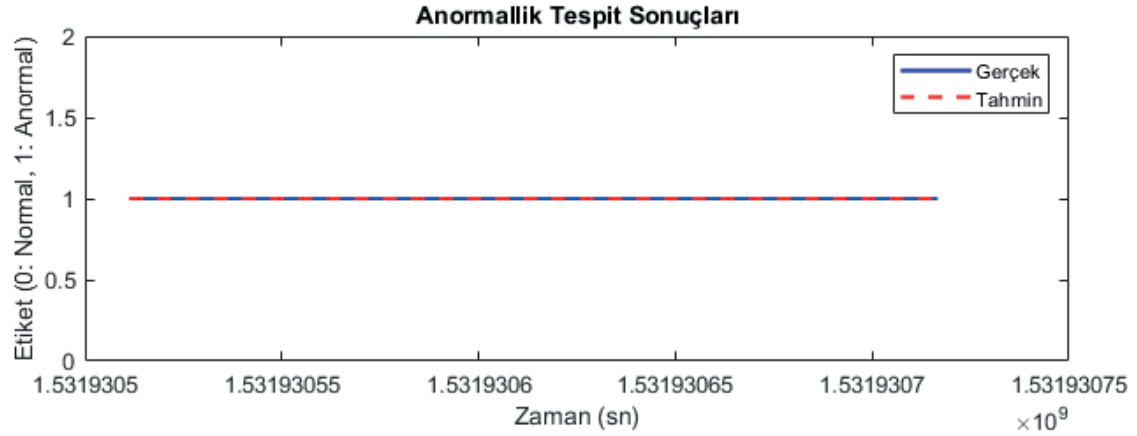
Bu bölümde, kanatçık arızalarına ait uçuş günlükleri verileri için gerçekleştirilen OC-SVM modelinin sonuçlarına benzer bir yaklaşım, dümen arızaları için uçuş günlükleri verileri üzerinde de uygulanmıştır. Eğitim aşamasında kullanılan model ve parametreler arıza verilerine de uyarlanarak model yeniden eğitilmiştir. Test verisinin boyutunun 4000 x 18 olduğu göz önünde

bulundurulduğunda, modelin farklı boyutlu ve farklı bir veri kümesi üzerinde test edildiğini ve sonuçların yine de %100 başarı oranıyla sonuçlandığını gösterdiği görülmektedir.

Şekil 5.9 ve Şekil 5.10'da sırasıyla, yeniden örneklenmiş bir özellik zaman serisi ve elde edilen test sonuçları görülmektedir.



Şekil 5.9. Yeniden örneklenmiş dümen arızası zaman serisi



Şekil 5.10. Dümen arızasına ait gerçek ve tahmin edilen OC-SVM sonuçları.

Hassasiyet, duyarlılık, F1-Skoru ve doğruluk ölçütleri için hesaplanan değerler yine tamamıyla 1 olarak elde edilmiştir. Bu durum, OC-SVM modelinin hem Kanatçık Arızaları hem de Dümen Arızaları verileri üzerinde yüksek başarı oranları elde ettiğini ve iki farklı arıza türü için de güvenilir bir sınıflandırma sağladığını göstermektedir. Dümen arızası test sonuçları için elde edilen performans metrikleri Tablo 5.3'te gösterilmektedir.

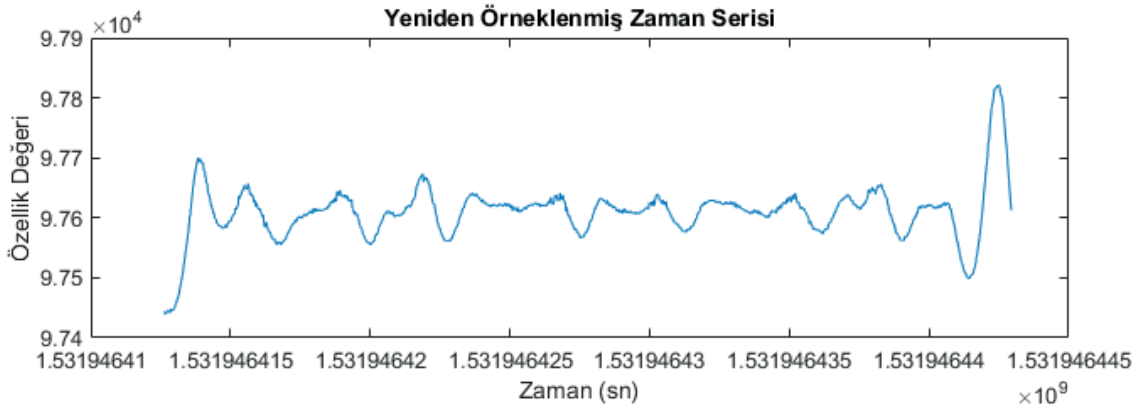
Tablo 5.3. Dümen arızası için OC-SVM performans değerlendirmesi

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

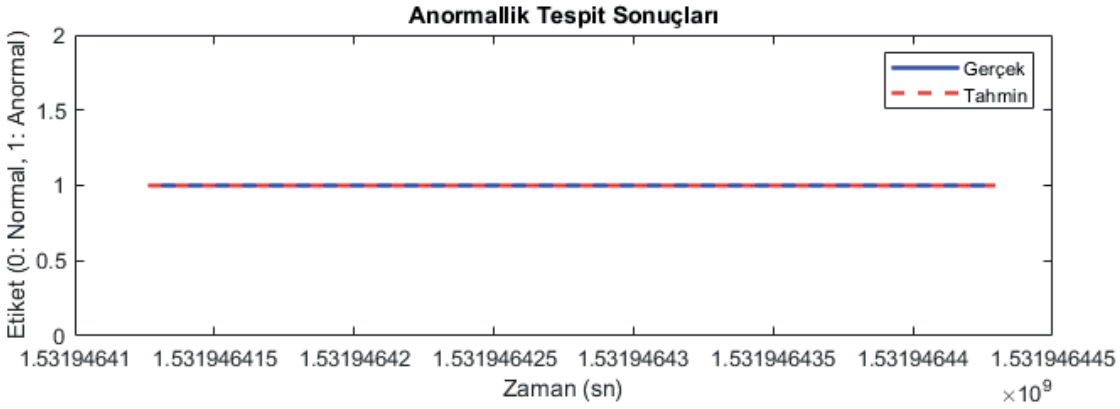
Elde edilen sonuçlar, modelin genel bir uygulamada gerçek zamanlı arıza tespitine yönelik etkili bir araç olarak kullanılma potansiyelini vurgulamaktadır. Bu çalışma, dümen arızaları verileri için elde edilen yüksek performanslı sonuçlarla, OC-SVM modelinin geniş bir aralıktaki arıza türleri için başarılı bir araç olarak değerlendirilmesini desteklemektedir. Veri setinin büyüklüğüne rağmen modelin %100 başarı elde etmesi, modelin veri setinin boyutuna bağımsız olarak istikrarlı bir performans sergilediğini göstermektedir.

5.3.4. OC-SVM ile Asansör Arızalarının Tespiti

Bu bölümde, asansör arızası için uçuş günlükleri verileri üzerinde de bir test yapılmıştır. Bu test, 2000 adet veri örneği ve 18 özellik parametresi ile gerçekleştirilmiştir. Şekil 5.11 ve Şekil 5.12'de sırasıyla bu arıza tipine ait bir özellik zaman serisi ve elde edilen test sonuçları görülmektedir.



Şekil 5.11. Yeniden örneklenmiş asansör arızası zaman serisi



Şekil 5.12. Asansör arızasına ait gerçek ve tahmin edilen OC-SVM sonuçları.

Elde edilen sonuçlar incelendiğinde, modelin arıza verileri üzerinde de yine %100 başarı oranı elde ettiği gözlemlenmiştir. Hassasiyet, duyarlılık, F1-Skoru ve doğruluk ölçütleri için hesaplanan değerler, testin her bir ölçüte göre tamamıyla 1 olduğunu göstermiştir.

Bu durum, OC-SVM modelinin farklı arıza türleri, farklı veri boyutları ve farklı veri miktarlarına bağımsız olarak yüksek performans sergilediğini göstermektedir.

Bu çalışma, OC-SVM modelinin uçuş günlükleri verilerini farklı arıza türleri için sınıflandırmada etkili bir araç olarak kullanabileceğini göstermektedir. Modelin %100 başarı elde ettiği bu testler, modelin güvenilirliğini ve genel uygulanabilirliğini desteklemektedir. Sonuç olarak, OC-SVM modeli, farklı arıza türlerinde ve farklı veri koşullarında başarılı sonuçlar elde edebilen bir araç olarak öne çıkmaktadır. Asansör arızası için elde edilen performans metrikleri Tablo 5.4'te gösterilmektedir.

Tablo 5.4. Asansör arızası için OC-SVM performans değerlendirmesi

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

5.4. Tek Sınıflı Rastgele Orman Sınıflandırıcısı ile Anormallik Tespiti

Tek Sınıflı Rastgele Orman Sınıflandırıcısı (OC-RF), anormallik tespiti veya aykırı değer tespiti gibi problemler için geliştirilmiş bir makine öğrenmesi algoritmasıdır. Bu algoritma, geleneksel Rastgele Orman (RF) algoritmasının bir varyasyonudur ve tek sınıflı veri kümeleri için özel olarak tasarlanmıştır.

Geleneksel RF algoritması, birçok karar ağacının (decision trees) topluluk olarak kullanıldığı bir sınıflandırma yöntemidir. Bu ağaçlar, rastgele seçilen özelliklerin alt kümeleri üzerinde bağımsız olarak eğitilmekte ve bir veri noktasının sınıfını tahmin etmek için bu ağaçlardan gelen oyları kullanılmaktadır. Her ağacın tahminleri bir araya getirilerek son tahmin yapılmaktadır.

RF algoritması, Leo Braiman ve Adele Cutler tarafından önerilen karar ağaçları topluluğuna dayalı algoritmadır [35]. Karar ağacı, bir nesnenin sınıflandırılmasını sağlamak için kullanılan bir mantık yapısıdır. Bu yapının temeli, hiyerarşik olarak düzenlenmiş bir soru sistemidir. Bir karar ağacı, "yapraklar" ve "dallar" adı verilen bileşenlerden oluşmaktadır. "Dallar", fonksiyonun bağımlı olduğu nitelikleri temsil ederken, "yapraklar" ise hedef etiketin değerlerini içermektedir. Ayrıca, her bir düğümdeki sorular, önceki cevaplara ve hiyerarşik düzeye bağlı olarak belirlenmektedir.

Karar ağacı, nesnelerin sınıflandırılması için bir yol haritası gibi işlev görmektedir. Başlangıç düğümü olan kök düğümünden başlayarak, her düğümdeki kararlar, özelliklerin değerlerine göre alınmakta ve ağacın dallarına ilerlemektedir. Her düğüm, bir özellikle ilgili bir soruyu temsil etmekte ve o özelliğin değerine bağlı olarak bir sonraki düğümü seçmektedir. Bu süreç, yaprak düğümlerine ulaşana kadar devam etmektedir. Yaprak düğümler, sınıf etiketlerini temsil etmekte ve nesnelerin sınıflandırıldığı son noktadır.

Karar ağacının oluşturulması, özelliklerin ve sınıfların bir veri setine göre analiz edilmesini gerektirmektedir. Her özellik, veri setindeki farklı değerlerine göre ayrıştırma yapmayı sağlamaktadır. Örnek olarak, bir karar ağacı, bir meyvenin türünü belirlemek için meyvenin rengini, şeklini ve dokusunu kullanabilmektedir. Bu durumda, renk bir düğümü, şekli bir başka düğümü ve dokusu bir başka düğümü temsil etmektedir. Bu özelliklere dayalı olarak, ağaç meyvenin hangi tür olduğunu belirlemek için ilerlemektedir.

Karar ağacı, sınıflandırma problemlerini çözmek için yaygın olarak kullanılan bir algoritmadır. Veri setindeki özelliklerin ve sınıfların öğrenilmesiyle, bir karar ağacı modeli oluşturulmaktadır. Bu model, yeni örneklerin sınıflandırılması için kullanılmaktadır. Karar ağacı, kolayca yorumlanabilen ve açıklanabilen bir yapıya sahip oluşturulmaktadır. Ayrıca, büyük veri kümeleri üzerinde etkili bir şekilde çalışabilmekte ve diğer sınıflandırma yöntemlerine kıyasla hızlı sonuçlar sağlayabilmektedir.

Karar ağacı, hastalık teşhisi, müşteri profili, spam filtreleme gibi birçok farklı alanda kullanılan bir sınıflandırma aracı olmaktadır. Özellikle, özelliklerin belirli bir hiyerarşik yapıya sahip olduğu ve sınıfların ayrımının net bir şekilde yapılabildiği problemlerde etkili olmaktadır. Ancak, veri setindeki gürültü, eksik veri veya dengesizlik gibi faktörler, karar ağacının performansını etkilemektedir. Bu nedenle, veri ön işleme adımları ve ağaç oluşturma parametrelerinin dikkatli bir şekilde seçilmesi gerekmektedir.

Karar ağacı, nesnelerin sınıflandırılması için kullanılan bir yöntemdir. Hiyerarşik yapıya sahip sorular ve cevaplarla birlikte özelliklere dayalı kararlar almaktadır. Bu yapısıyla, anlaşılır ve

açıklanabilir sonuçlar üretebilmektedir. Karar ağacı, geniş bir uygulama alanına sahip olan etkili bir sınıflandırma aracıdır ve veri analitiği ve makine öğrenimi alanında sıkça kullanılmaktadır.

Veri sınıflandırmadan önce, bir karar ağacı sınıflandırıcısını eğitmek gerekmektedir. Eğitim süreci, analiz edilen veri setinden rastgele örneklerin seçildiği bir eğitim seti kullanılarak gerçekleştirilmektedir. Eğitim, en uygun eşik parametre değerlerinin belirlenmesi veya özelliklerin ikili olarak bölünmesini içermektedir. Bu amaçla, alt kümelerdeki heterojenleri ölçmek için genellikle entropi indeksi gibi bir değer kullanılmaktadır.

Karar ağacının inşası, veri setindeki her bir özelliğin entropi değerlerine dayanarak gerçekleştirilmektedir. İlk olarak, setin tamamına ait bir kök düğümü oluşturulmakta ve en uygun özellik seçilmektedir. Bu seçim, alt kümelerin en iyi şekilde ayrıştırılabileceği özelliği temsil etmektedir. Daha sonra, veri seti bu özelliğe göre alt kümeler halinde bölünmekte ve bu bölünme süreci, alt kümelerin her biri için aynı şekilde tekrarlanır, yani alt kümeler kendi içinde en iyi özelliğe göre bölünmektedir.

Bölünme süreci, belirli bir durma kriteri sağlanana kadar devam etmektedir. Bu kriter, bir alt kümenin tam tekdüzeliği sağladığı veya sınıf etiketlerine göre tam olarak ayrıldığı durumu ifade etmektedir. Yani, alt kümeler bir sınıfa ait tüm örnekleri içerdiğinde veya alt kümelerdeki örnekler tam olarak bir sınıfa ait olduğunda bölünme durmakta ve bu alt kümeler "yaprak" düğümleri olarak adlandırılmaktadır.

Önemli bir nokta, eğitim setinde farklı sınıflara ait her özellik için aynı değere sahip nesnelerin bulunmaması gerekmektedir. Bu, ağacın her zaman bir karar noktasına ulaşabileceği anlamına gelmektedir. Aksi takdirde, bir özelliğin değerine dayalı olarak hiçbir ayrıştırma yapılamamakta ve karar ağacı oluşturulamamaktadır.

Sonuç olarak, karar ağacının eğitim süreci, veri setindeki özelliklerin ve sınıfların analiz edilmesini içermektedir. En uygun eşik değerlerini ve özelliklerin bölünme sırasını belirlemek için entropi gibi bir ölçütü Denklem 5.6'daki gibi heterojenliğin entropi indeksi olarak kullanılmaktadır. Ağaç, özelliklere dayalı olarak alt kümeler halinde bölünerek inşa edilmektedir. Bu süreç, belirli bir durma kriterine ulaşıncaya kadar devam etmekte ve sonuç olarak anlaşılabilir ve açıklanabilir bir karar ağacı oluşturulmaktadır.

$$\gamma_e = -\sum_{i=1}^{L} P_l * In(P_l) \tag{5.6}$$

$$\gamma_g = 1 - \sum_{i=1}^{L} P_l^2 \tag{5.7}$$

P_l, nesnelerin oranıdır, γ_e, heterojen entropi indeksi maksimuma çekilmekte, Denklem 5.7'de γ_g, indeksi de minimuma çekilmektedir [35].

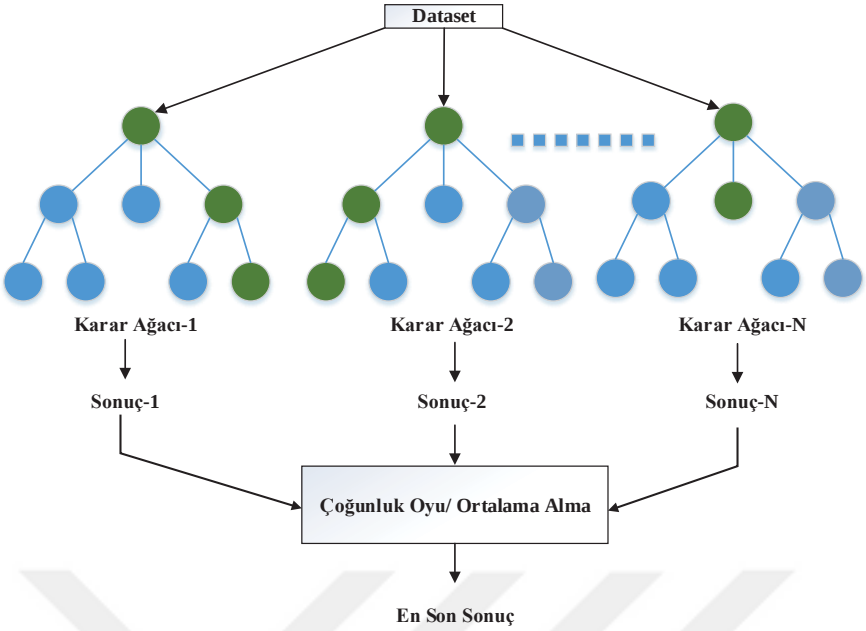
OC-RF, geleneksel RF algoritmasından farklı olarak tek sınıflı veri kümeleri için kullanılmaktadır. Bu durumda, sadece normal örneklerin olduğu bir sınıf etiketi bulunurken, anormal veriler etiketlenmez veya dikkate alınmamaktadır. Anormal örnekler genellikle normal verilere göre nadir ve farklı davranışları temsil etmektedir.

OC-RF'nin temel amacı, normal verileri temsil eden bir model oluşturarak geri kalan verileri bu modele göre anormallik olarak sınıflandırılmaktadır. Bu sayede, normal verilerden sapma gösteren anormal verileri tespit etmek mümkün hale gelmektedir.

Anormallik tespiti, genellikle veri setindeki normal davranışın ötesindeki nadir veya anormal örneklerin tanımlanmasıyla ilgilidir. Bu, birçok alanda önemli bir sorundur, örneğin sahtekârlık tespiti, ağ güvenliği, tıbbi teşhis ve endüstriyel hata tespiti gibi alanlarda kullanılmaktadır. OC-RF bu tür sorunları çözmek için etkili bir çözüm sunmaktadır.

$$f(x) = \frac{1}{B}\sum_{i=1}^{B} t^i(x^i) \tag{5.8}$$

Denklem 5.8'de B, öyküleme kopyalarının sayısıdır, $t^i(x^i)$, öyküleme örnekleminin i üzerinde inşa edilen ağaçtır. Optimal azaltma, ağaçların her biri bağımsız olduğunda gerçekleşmektedir. Ancak çoğu durumda önyüklemeli örnek üzerine inşa edilen ağaçlar benzer olma eğilimindedir. Ağaçlar arasındaki korelasyonu en aza indirmek için rastgele ormanlar yöntemi kullanılmaktadır. Her ağaç için yeni bir uç düğüm oluştururken ortak değişkenlerin yalnızca rastgele bir alt kümesini kullanılmaktadır. Bir ağaç inşa etmede kullanılan ilave rastgele oluşturulan bir değer ile birlikte ağaçların üzerinde torbalama işlemi gerçekleşmektedir. Rastgele ormanların, düşük genelleme hatasını korurken geniş bir işlev sınıfına yaklaşmasını sağlamaktadır [36]. Şekil 5.13'te OC-RF modelinin şematik gösterimi görülmektedir.



Şekil 5.13. Tek sınıflı rastgele orman algoritması.

Bu bölümde, OC-RF yöntemi kullanılarak gerçekleştirilen arıza tespit çalışmasının sonuçları ayrıntılı bir şekilde sunulmuştur. Eğitim aşamasında 10,000 adet güvenli uçuş (normal veri) örneği kullanılmıştır. Test aşamasında ise farklı arıza türlerini temsil eden toplam 37,000 adet arızalı uçuş örneği test edilmiştir. Her bir veri seti 18 parametre içermekte olup, bu parametreler uçuş günlüklerinden seçilmiştir.

OC-RF'nin bazı avantajları şunlardır:

- Tek sınıflı bir model olduğu için anormallik tespiti için ayrı bir anormallik sınıfı etiketi gerektirmemektedir.
- Geleneksel RF algoritmasının güçlü yanlarından biri olan yüksek doğruluk ve direnç özelliklerini korumaktadır.
- Özellikle nadir ve karmaşık anormalliklerin tespiti için etkilidir.

Ancak, OC-RF'nin bazı sınırlamaları da vardır.

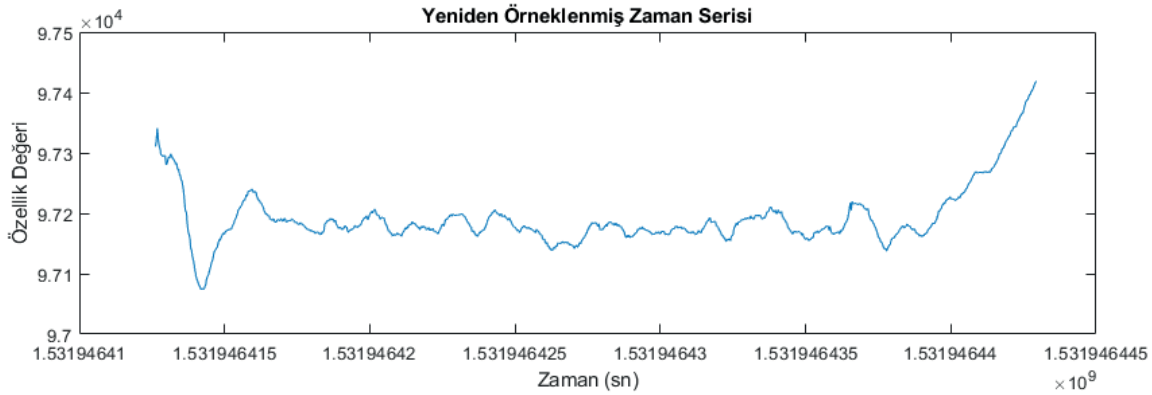
- Anormallik tespiti için yalnızca normal verilerin kullanılması nedeniyle anormalliklerin tam bir temsili zor olmaktadır.
- Eşik değeri seçimi önemlidir ve bazen uygun bir eşik değeri bulmak zor olmaktadır.
- Veri dengesizlikleri durumunda performansı etkilenebilmektedir. Örneğin, normal veriler anormallere kıyasla çok daha fazlaysa, model normal verileri yanlışlıkla anormallik olarak sınıflandırılmaktadır.

Bu bilgiler, OC-RF'nin temel çalışma prensipleri ve avantajları hakkında bir genel bakış sağlamaktadır. Anormallik tespiti, çok çeşitli uygulama alanlarında kullanılabilen bir tekniktir ve

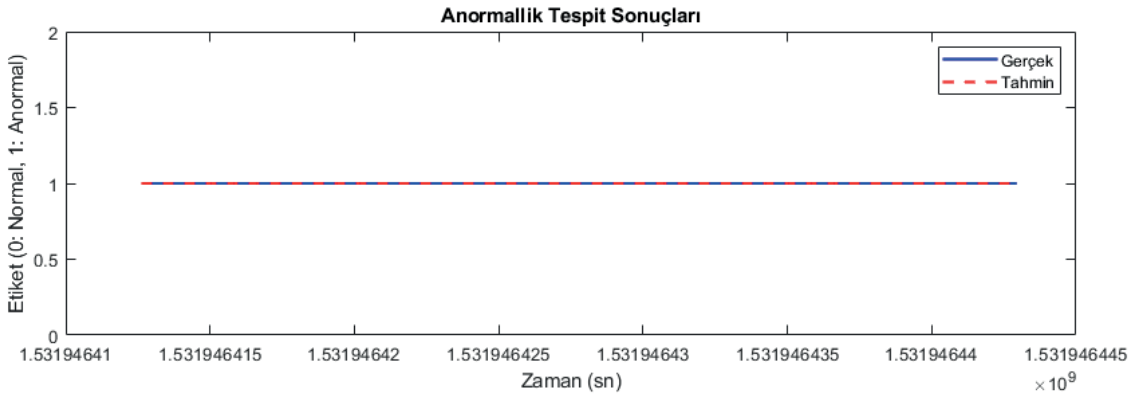
OC-RF bu tür problemlerin çözümünde etkili bir araç olarak değerlendirilmektedir. Ancak, her bir uygulama senaryosunda OC-RF'nin avantajları ve sınırlamaları dikkate alınmalıdır.

5.4.1. OC-RF ile Motor Arızalarının Tespiti

Şekil 5.14'te, motor arızası tespitinde kullanılan örnek bir zaman serisi görülmektedir. Motor arızalarının tespit sonuçları ise Şekil 5.15'de sunulmuştur. Motor arızası tespiti için yapılan testlerde, OC-RF yöntemi %100 başarı oranı elde etmiştir. Bu sonuçlar, motor arızalarının güvenilir bir şekilde tespit edildiğini ve modelin motor arızalarını kesin bir doğrulukla tanımlayabildiğini göstermektedir.



Şekil 5.14. Yeniden örneklenmiş motor arızası zaman serisi



Şekil 5.15. Motor arızasına ait gerçek ve tahmin edilen OC-RF sonuçları.

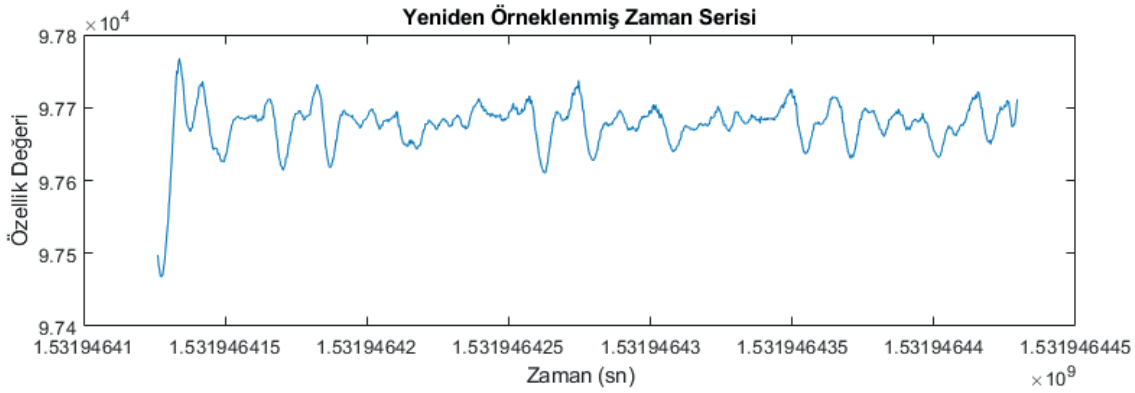
Hassasiyet, duyarlılık, F1 skoru ve doğruluk metriklerinin tamamı 1 olarak hesaplanmıştır, bu da modelin motor arızalarını yanlış pozitif veya yanlış negatif sonuçlar vermeden doğru bir şekilde tespit ettiğini göstermektedir. Motor arızasında performans değerlendirmesi Tablo 5.5'te gösterilmektedir.

Tablo 5.5. Motor arızası için OC-RF performans değerlendirmesi

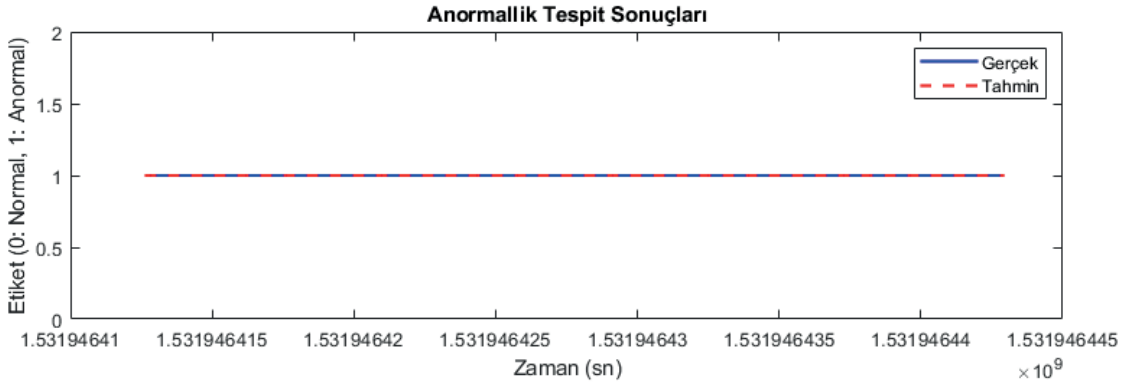
Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

5.4.2. OC-RF ile Kanatçık Arızalarının Tespiti

Kanatçık arızalarının tespiti için kullanılan yeniden örneklenmiş bir özellik zaman serisi Şekil 5.16'da tespit sonuçları ise Şekil 5.17'de görülmektedir. Kanatçık arızası tespiti için yapılan testlerde de OC-RF yöntemi %100 başarı oranı elde etmiştir. Bu durum, modelin kanatçık arızalarını da aynı şekilde doğru bir şekilde tespit ettiğini göstermektedir.



Şekil 5.16. Yeniden örneklenmiş kanatçık arızası zaman serisi



Şekil 5.17. Kanatçık arızasına ait gerçek ve tahmin edilen OC-RF sonuçları.

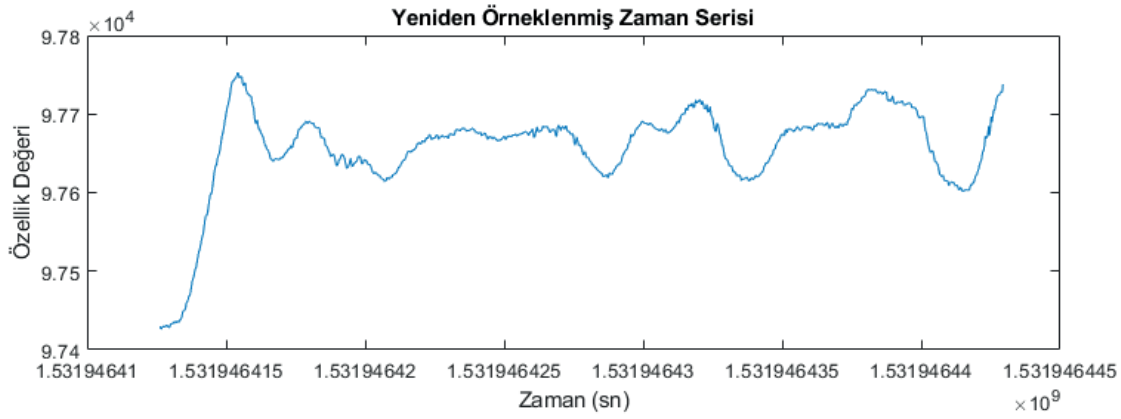
Performans değerlendirme metriklerinin tamamının 1 olarak hesaplanması, modelin kanatçık arızalarını yanlış sınıflandırmadan kesin bir şekilde tanımlayabildiğini göstermektedir. Kanatçık arızası için hesaplanan performans metrikleri Tablo 5.6'da görülmektedir.

Tablo 5.6. Kanatçık arızası için OC-RF performans değerlendirmesi

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

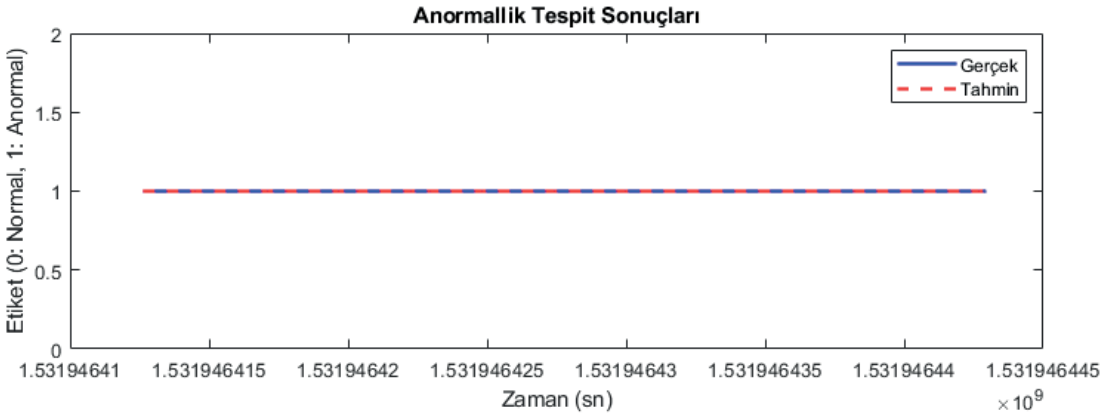
5.4.3. OC-RF ile Dümen Arızalarının Tespiti

Dümen arızalarının tespiti için kullanılan yeniden örneklenmiş bir özellik zaman serisi Şekil 5.18'de, tespit sonuçları ise Şekil 5.19'da görülmektedir.



Şekil 5.18. Yeniden örneklenmiş dümen arızası zaman serisi

Dümen arızası tespit sonuçları, OC-RF yönteminin bu tür arızaları yüksek bir doğrulukla tespit ettiğini göstermektedir. Hassasiyet ve duyarlılık değerlerinin her ikisi de 1 olarak hesaplanmıştır, bu da modelin hem arıza varlığını doğru bir şekilde belirlediğini hem de sağlıklı uçuş durumlarını yanlış pozitif sonuçlarla karıştırmadan doğru bir şekilde sınıflandırdığını göstermektedir. F1 skoru da 1 olarak hesaplandığından, modelin kesin sonuçlar ürettiği ve dengeli bir tespit yeteneğine sahip olduğu söylenebilir.



Şekil 5.19. Dümen arızasına ait gerçek ve tahmin edilen OC-RF sonuçları.

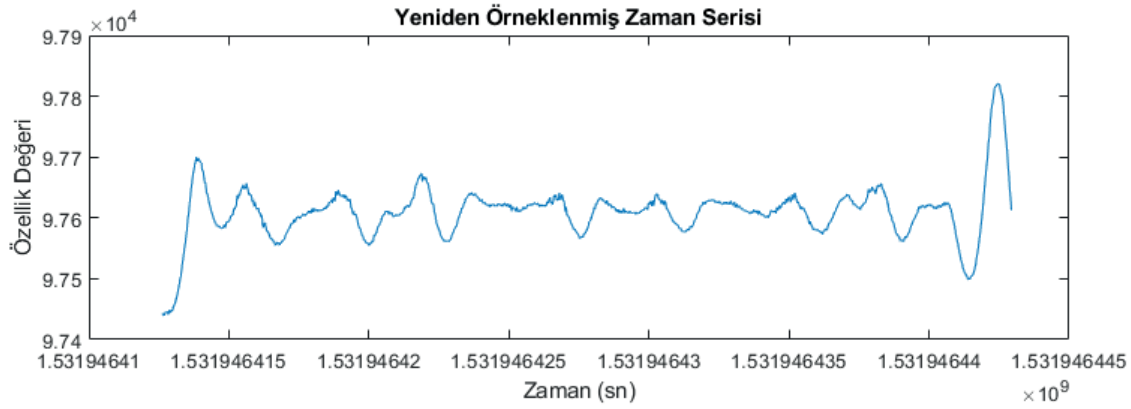
Dümen arızası tespitinde elde edilen performans metrik değerleri Tablo 5.7'de gösterilmektedir. Bu sonuçlar, dümen arızaları için OC-RF yönteminin güvenilir ve etkili bir arıza tespit yöntemi olduğunu desteklemektedir.

Tablo 5.7. Dümen arızası için OC-RF performans değerlendirmesi

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

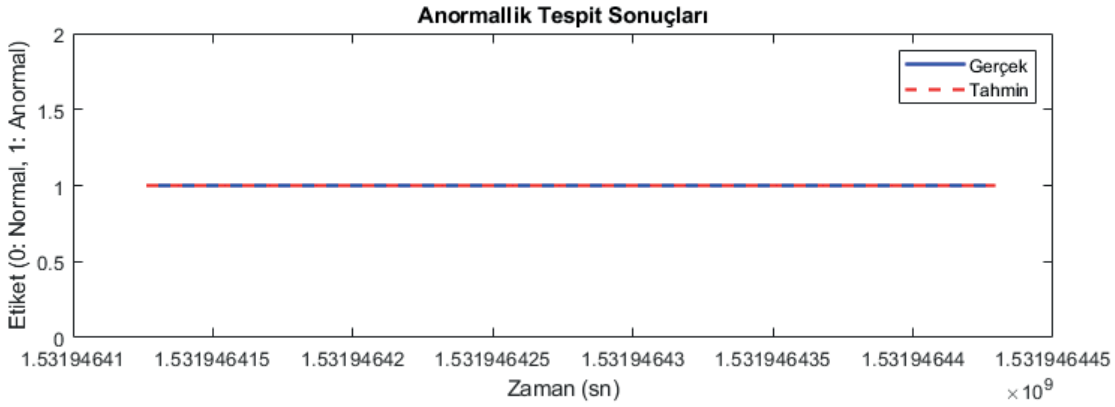
5.4.4. OC-RF ile Asansör Arızalarının Tespiti

Asansör arızalarının tespitinde kullanılan örnek bir zaman serisi Şekil 5.20'de görülmektedir. Asansör arızalarının tespit sonuçları ise Şekil 5.21'de sunulmuştur. Asansör arızaları tespit sonuçları, OC-RF yönteminin bu tür arızaları da yüksek bir doğrulukla tespit ettiğini göstermektedir. Hassasiyet ve duyarlılık değerlerinin her ikisi de 1 olarak hesaplanmıştır, bu da modelin hem arıza varlığını doğru bir şekilde belirlediğini hem de sağlıklı uçuş durumlarını yanlış pozitif sonuçlarla karıştırmadan doğru bir şekilde sınıflandırdığını göstermektedir. F1 skoru da 1 olarak hesaplandığından, modelin kesin sonuçlar ürettiği ve dengeli bir tespit yeteneğine sahip olduğu söylenebilir. Bu sonuçlar, Asansör arızaları için OC-RF yönteminin güvenilir ve etkili bir arıza tespit yöntemi olduğunu desteklemektedir.



Şekil 5.20. Yeniden örneklenmiş asansör arızası zaman serisi

Asansör arızası anomali tespitinde kullanılan 2000 adet arızalı verinin tamamı doğru olarak tahmin edilmiştir.



Şekil 5.21. Asansör arızasına ait gerçek ve tahmin edilen OC-RF sonuçları.

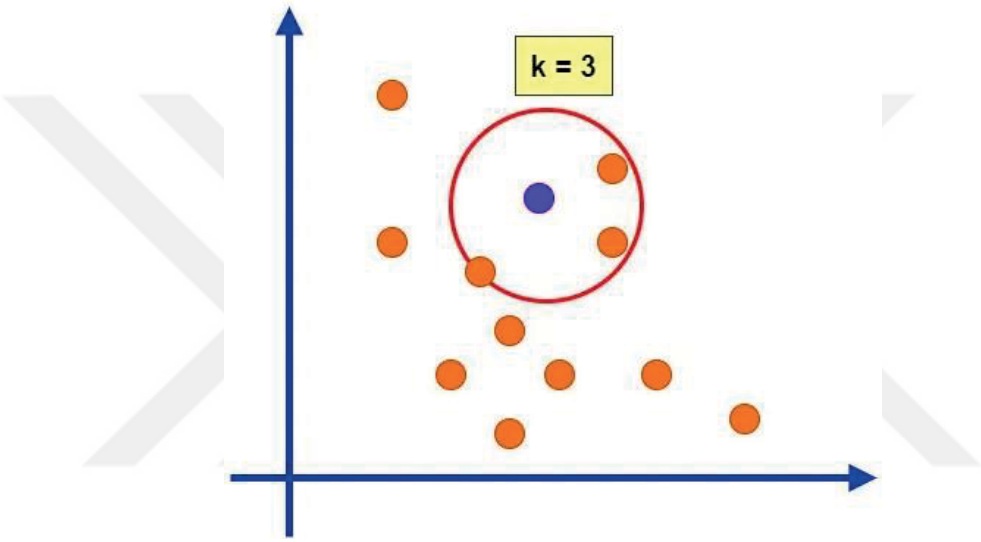
Asansör arızasında test sonuçları için hesaplanan performans metrikleri ve değerleri Tablo 5.8'de gösterilmektedir.

Tablo 5.8. Asansör arızası için OC-RF performans değerlendirmesi

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

5.5. Yerel Aykırı Faktör ile Anormallik Tespiti

Yerel Aykırı Faktör (Local Outlier Factor - LOF), Local Outlier Factor (LOF), aykırı değer tespiti için kullanılan bir algoritmadır ve veri noktalarının lokal yoğunluğunu değerlendirerek aykırı değerleri tespit etmeyi amaçlar. LOF algoritması, her bir veri noktasının etrafındaki çevresel yapıyı analiz ederek, diğer noktalardan olan uzaklığına göre bir aykırılık skoru hesaplar. Bu skor, bir veri noktasının aykırılığını ölçmeye yardımcı olur [37]. Şekil 5.22'de gösterilen merkezdeki nokta ele alındığında k = 3 için en yakın 3 komşuluğuna bakılmaktadır. Bu durum daire içerisine alınarak gösterilmiştir.



Şekil 5.22. k-uzaklığı (k = 3)

LOF algoritmasının temel adımları aşağıdaki gibidir:

1. **K-En Yakın Komşuların Belirlenmesi:** Her veri noktası için, belirli bir K sayısıyla en yakın K komşusu belirlenir. Bu komşuluk, veri noktasının lokal çevresini yakalamak amacıyla kullanılır.
2. **Lokal Yoğunluğun Hesaplanması:** Her veri noktasının etrafındaki lokal yoğunluk, K-en yakın komşularının uzaklıkları kullanılarak hesaplanır. Daha fazla veri noktasının yakınlık içerisinde ise bu noktanın lokal yoğunluğu yüksek olur.
3. **LOF Değerinin Hesaplanması:** Bir veri noktasının LOF değeri, onun lokal yoğunluğunun K-en yakın komşularının lokal yoğunluklarına oranı olarak hesaplanır. Eğer bir veri noktasının LOF değeri 1'e yakınsa, bu nokta diğer veri noktalarıyla benzer bir çevresel yapıya sahiptir. Ancak LOF değeri 1'den uzaklaştıkça, bu noktanın çevresindeki yoğunluğun diğer veri noktalarından farklı olduğu anlaşılır ve aykırı değer olarak değerlendirilebilir.

Matematiksel olarak LOF değeri (LOF_k(x)) aşağıdaki formülle ifade edilir [38]:

$$LOF_k(x) = \frac{\sum_{o \epsilon N_k(x)} \frac{lrd(o)}{lrd(x)}}{k} \quad (5.9)$$

Burada: $N_k(x)$, x veri noktasının en yakın k komşusunu ifade eder. lrd(x) ise, x veri noktasının lokal yoğunluğunu ifade eder. Bu yöntem, aykırı değerleri tespit etme açısından etkili bir yaklaşımdır ve çeşitli uygulama alanlarında kullanılmaktadır.

LOF skoru, bir veri noktasının anormallik düzeyini temsil eder. LOF skoru yüksek olan noktalar, çevresindeki diğer noktalardan belirgin bir şekilde farklıdır ve bu nedenle anormal olarak kabul edilir. LOF skorlarına göre noktalar sıralanabilir ve en yüksek LOF skorlarına sahip olanlar en anormal olarak kabul edilmektedir.

LOF algoritmasının avantajlarından bazıları şunlardır:

- Veri setinin yapısına bağımlı olmaksızın çalışabilmesi.
- Aykırı değerleri tespit etmek için genel bir yöntem sunması.
- Çok boyutlu veri kümelerinde etkili bir şekilde çalışabilmesi.
- Gürültülü verilere karşı dirençli olabilmesi.

Ancak, LOF algoritmasının bazı zorlukları da vardır:

- Büyük veri setlerinde hesaplama maliyeti yüksek olabilir.
- Optimal komşuluk parametresini belirlemek zor olabilir.
- Veri setinde homojen bölgeler varsa yanlı sonuçlar üretebilir.

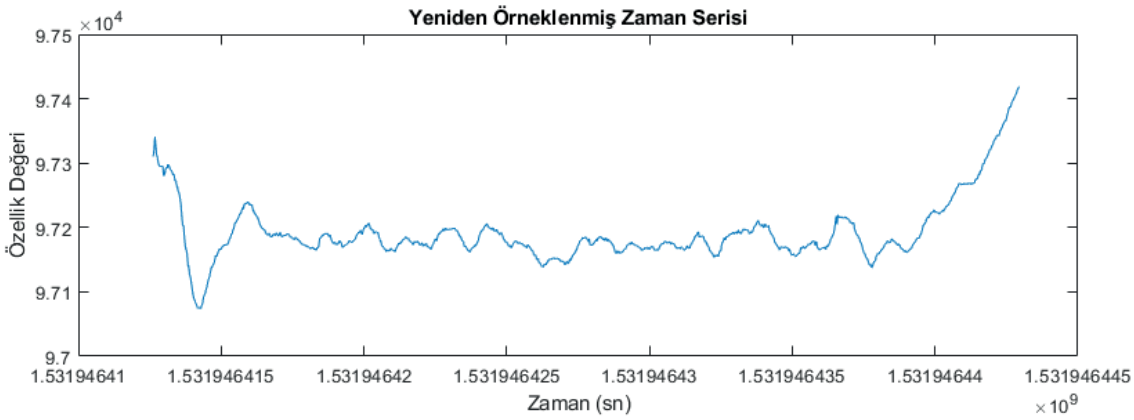
LOF algoritması, birçok alanda kullanılabilmektedir. Örneğin, dolandırıcılık tespiti, ağ güvenliği, sağlık analitiği, kalite kontrol, coğrafi bilgi sistemleri gibi alanlarda LOF'un anomali tespitinde etkili olduğu görülmüştür.

Sonuç olarak, LOF algoritması, bir veri noktasının çevresindeki diğer noktalarla karşılaştırılarak ne kadar anormal olduğunu ölçen bir anomali tespit algoritmasıdır. Bu algoritmanın çalışma prensipleri, avantajları ve zorlukları, veri madenciliği ve makine öğrenmesi alanlarında geniş bir kullanım alanına sahip olduğunu göstermektedir.

5.5.1. LOF ile Motor Arızalarının Tespiti

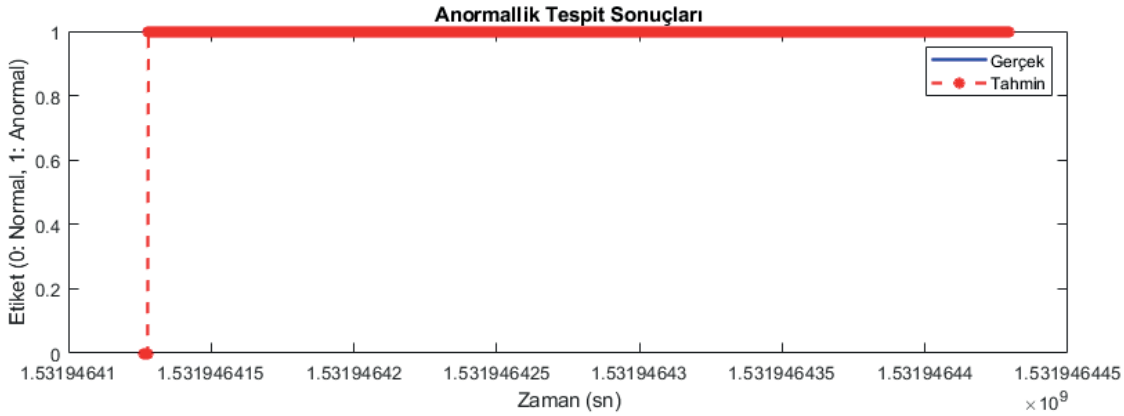
LOF ile eğitim aşamasından sonra yeniden örneklenmiş zaman serisi örnekleri kullanılarak yapılan test işleminde başarı oranı %99,95 olarak elde edilmiştir.

Şekil 5.23'de, test işleminde kullanılan zaman serisi örneklerinden biri görülmektedir.



Şekil 5.23. Yeniden örneklenmiş motor arızası zaman serisi

Motor arızası anomali tespitinde kullanılan 23.000 adet arızalı verinin 22.994'ü de doğru ve 6'sı yanlış olarak tahmin edilmiştir. Elde edilen sonuçlar Şekil 5.24'te gösterilmektedir.



Şekil 5.24. Motor arızasına ait gerçek ve tahmin edilen OC-RF sonuçları.

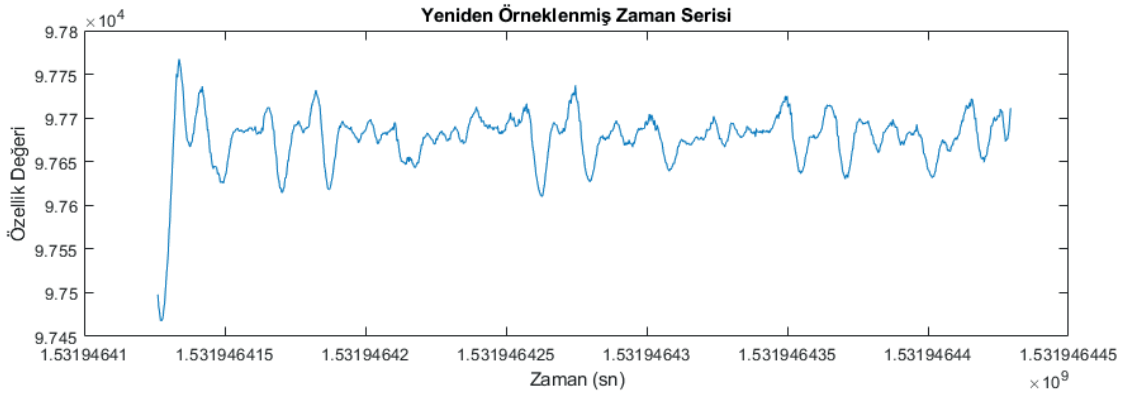
Motor arızası tespiti için yapılan LOF test işlemi sonucunda hesaplanan performans metrikleri Tablo 5.9'da gösterilmektedir. Bu yöntem ile elde edilen arıza tespit sonuçlarına bakıldığında her ne kadar yüksek bir başarı oranı elde edilmiş olsa da OC-SVM ve OC-RF yöntemlerine göre doğruluk, duyarlılık ve F1-skor performans değerlendirme metriklerinin daha düşük olduğu görülmektedir. Öte yandan yapılan benzetim çalışmasında varsayılan model parametrelerinin kullanıldığı göz önünde bulundurulduğunda, parametre optimizasyonu yapılarak daha iyi sonuçlar elde edilebileceği düşünülmektedir. Test işleminde kullanılan veri sayısı dikkate alındığında elde edilen sonuçların tatmin edici olduğu görülmektedir.

Tablo 5.9. Motor arızası için LOF performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	0,99974
Hassasiyet (Precision)	1
Duyarlılık (Recall)	0,99974
F1-Ölçüsü (F1-Score)	0,99987

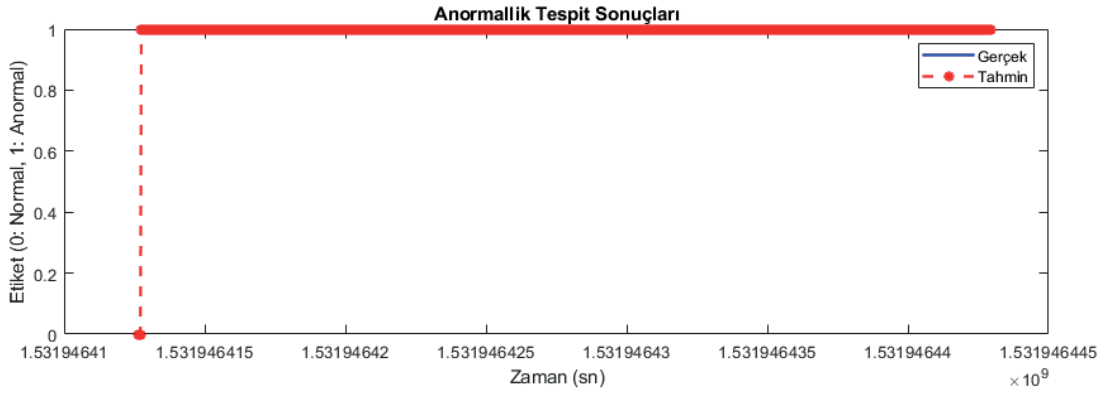
5.5.2. LOF ile Kanatçık Arızalarının Tespiti

Kanatçık arızası için LOF sınıflandırıcısı ile yapılan test işleminde başarı oranı %99,97 olarak bulunmuştur. Arıza tespitinde kullanılan ve arızalı durumda uçuş günlüklerinden alınan özellik zaman serisi Şekil 5.25'de görülmektedir.



Şekil 5.25. Yeniden örneklenmiş kanatçık arızası zaman serisi.

Kanatçık arızası anomali tespitinde kullanılan 8.000 adet arızalı verinin 7.996'sı doğru ve 4 tanesi ise yanlış olarak sınıflandırılmıştır. Test işlemi sonucunda elde edilen gerçek ve tahmin değerleri Şekil 5.26'da gösterilmektedir. Doğru olarak sınıflandırılan örnekler 1 (arızalı), yanlış olarak sınıflandırılan örnekler ise 0 (normal) olarak etiketlendirilmiştir.



Şekil 5.26. Kanatçık arızasına ait gerçek ve tahmin edilen OC-RF sonuçları

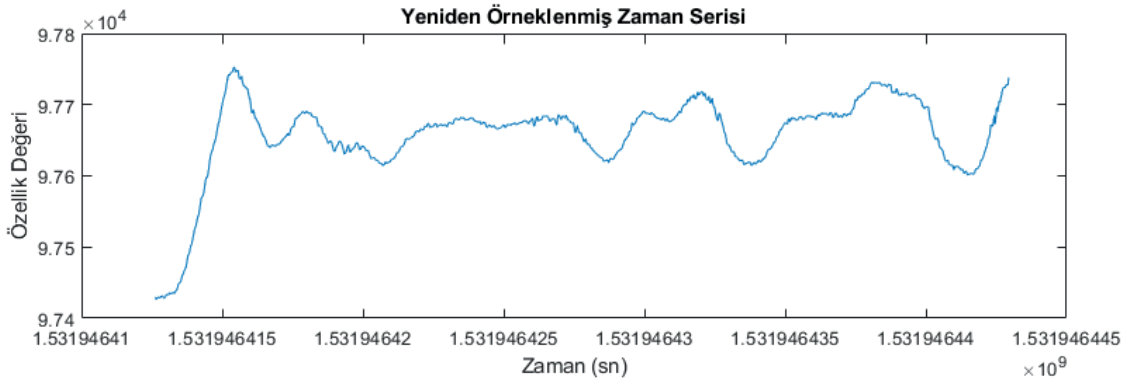
Kanatçık arızası için yapılan test işlemi sonucunda elde edilen LOF performans metrikleri Tablo 5.10'da gösterilmektedir. Elde edilen sonuçlara bakıldığında metrik değerlerinin 1'e oldukça yakın değerler aldıkları görülmektedir. Bu sonuçlar, LOF yönteminin anomali tespitinde kullanılabilecek alternatif bir yöntem olduğunu doğrulamaktadır.

Tablo 5.10. Kanatçık arızası için LOF performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	0,9995
Hassasiyet (Precision)	1
Duyarlılık (Recall)	0,9995
F1-Ölçüsü (F1-Score)	0,99975

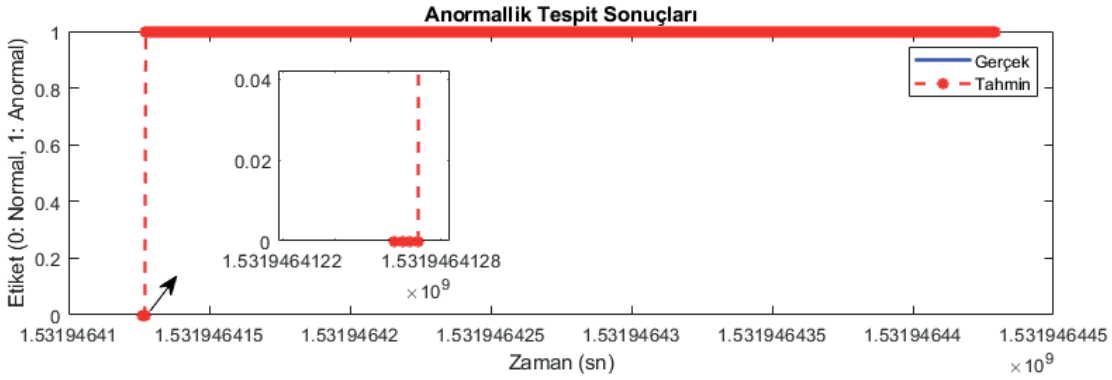
5.5.3. LOF ile Dümen Arızalarının Tespiti

Dümen arızasına ait veriler kullanılarak yapılan test işleminde LOF sınıflandırıcısının başarı oranı %99,97 olarak elde edilmiştir. Yeniden örneklendirilmiş özellik zaman serisi ve elde edilen test sonuçları sırasıyla Şekil 5.27 ve Şekil 5.28'de verilmiştir. Şekil 5.28'de arızalı (1) olduğu halde normal olarak (0) etiketlenen uçuş günlüğü verileri açık bir biçimde görülmektedir.



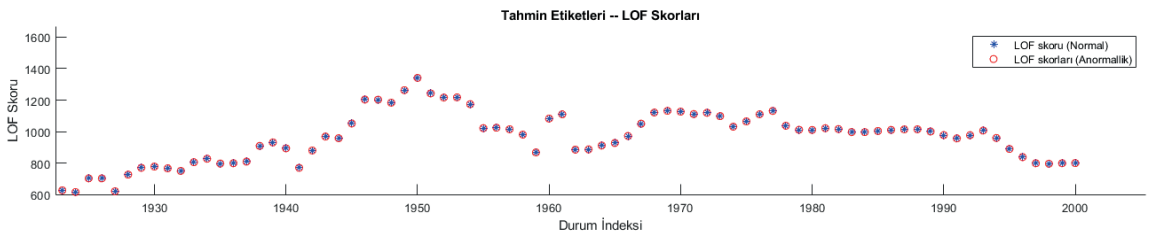
Şekil 5.27. Yeniden örneklenmiş dümen arızası zaman serisi

Dümen arızası anomali tespitinde kullanılan 4.000 adet arızalı verinin 3.996'sı doğru, 4'ü ise yanlış olarak tahmin edilmiştir.



Şekil 5.28. Dümen arızasına ait gerçek ve tahmin edilen OC-RF sonuçları

Dümen arızasında tahmin edilen LOF skoru değerleri Şekil 5.29'da gösterilmektedir.



Şekil 5.29. Tahmin edilen LOF skoru değerleri

Dümen arızası için elde edilen sınıflandırma sonuçlarının istatistiksel olarak değerlendirilebilmesi için hesaplanan performans ölçüm metrikleri Tablo 5.11'de gösterilmektedir.

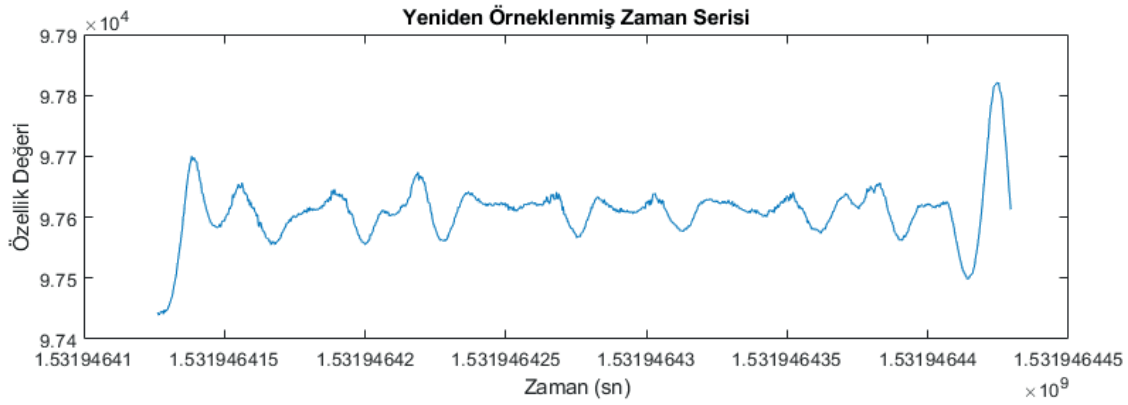
Tablo 5.11. Dümen arızası için LOF performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	0,999
Hassasiyet (Precision)	1
Duyarlılık (Recall)	0,999
F1-Ölçüsü (F1-Score)	0,9995

5.5.4. LOF ile Asansör Arızalarının Tespiti

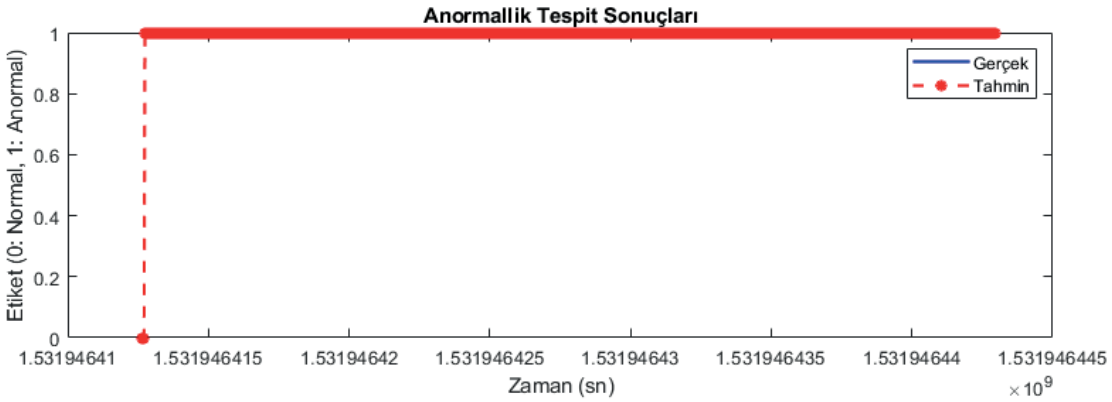
Son olarak, diğer sınıflandırma yöntemlerinde olduğu gibi asansör arızalarına ait uçuş günlükleri verileri test edilmiş ve LOF sınıflandırma yönteminin başarı oranı %99,90 olarak bulunmuştur.

Bu arıza tipine ait uçuş günlüğü veri seti içindeki yeniden örneklenmiş bir özellik zaman serisi Şekil 5.30'da görülmektedir.



Şekil 5.30. Yeniden örneklenmiş asansör arızası zaman serisi.

Asansör arızası anomali tespitinde kullanılan 2.000 adet arızalı verinin 1.996'sı doğru, 4'ü ise yanlış olarak tahmin etmiştir. Elde edilen sınıflandırma sonuçları Şekil 5.31'de görülmektedir.



Şekil 5.31. Asansör arızasına ait gerçek ve tahmin edilen OC-RF sonuçları.

Diğer arıza tiplerinde olduğu gibi bu arıza tipi için de istatistiksel performans değerlendirme metrikleri hesaplanmış ve elde edilen sonuçlar LOF sınıflandırma yönteminin bu arızaları yüksek doğrulukta ve güvenilirlikte tespit edebildiği sonucuna ulaşılmıştır. Elde edilen performans metrikleri Tablo 5.12'de gösterilmektedir.

Tablo 5.12. Asansör arızası için LOF performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	0,998
Hassasiyet (Precision)	1
Duyarlılık (Recall)	0,998
F1-Ölçüsü (F1-Score)	0,999

5.6. Otomatik Kodlayıcı ile Anormallik Tespiti

Anormallik tespiti, İHA'ların normal işleyişinden sapmaları veya saldırılara maruz kalmalarını tespit etmek için kullanılan bir tekniktir. Bu, İHA'ların normal davranışlarını belirlemek ve bunlardan sapmaları tespit etmekle ilgilidir. Otomatik kodlayıcı, bu amaçla etkili bir yöntem olarak öne çıkmaktadır.

Otomatik kodlayıcı, gözetimsiz bir öğrenme algoritmasıdır. Girdi verilerini sıkıştıran (enkoder) ve ardından orijinal veriyi yeniden oluşturan (dekoder) yapay sinir ağlarıdır. Otomatik Kodlayıcı, girdi verilerini temsil etmek ve özelliklerini çıkarmak için kullanılır. Bu özelliği, anormallik tespiti için kullanılabilir hale getirir.

Otomatik Kodlayıcı ile anormallik tespiti süreci aşağıdaki adımlardan oluşur:

- Anormallik tespiti için eğitim verileri toplanmalıdır. Bu veriler, normal İHA işleyişi sırasında toplanan ve etiketlenen verilerden oluşmaktadır. Eğitim verileri, İHA'nın normal

çalışmasını ve davranışını yansıtmaktadır. Bu adımda, İHA'nın normal davranışlarını temsil eden verilerin seçimi ve hazırlanması önemlidir.

- Eğitim verileri, Otomatik Kodlayıcı modeline verilerek eğitim süreci başlatılmaktadır. Otomatik Kodlayıcı, normal İHA verilerini kullanarak girdi verilerini sıkıştırmakta ve ardından orijinal veriyi yeniden oluşturmaktadır. Eğitim süreci boyunca, Otomatik Kodlayıcı modeli normal verilerdeki kalıpları ve yapıları öğrenmektedir. Bu sayede, model normal İHA işleyişini temsil eden bir içsel temsilasyon oluşturmaktadır.
- Otomatik Kodlayıcı, test verilerini kullanarak rekonstrüksiyon hatalarını hesaplamaktadır. Test verileri, normal İHA işleyişinden farklı olan verileri veya saldırı senaryolarını temsil edebilmektedir. Otomatik Kodlayıcı, test verisini kodlayıp, çözümlerken rekonstrüksiyon hatasını hesaplamaktadır. Rekonstrüksiyon hatası, gerçek ve tahmini veri arasındaki farkı ölçmektedir.

Otomatik Kodlayıcı, rekonstrüksiyon hatasını kullanarak anormallik tespiti yapmaktadır. Eğer test verisi, normal İHA verilerine benzemeyen bir şekilde yeniden oluşturuluyorsa, yani rekonstrüksiyon hatası yüksekse, bu veri anormal olarak kabul edilmektedir. Yüksek bir rekonstrüksiyon hatası, İHA üzerinde bir saldırı veya anormallik durumunun olduğunu gösterebilmektedir.

Otomatik Kodlayıcı ile anormallik tespiti, birçok avantaja sahiptir:

- Otomatik Kodlayıcı, gözetimsiz öğrenme algoritması olduğu için etiketlenmemiş verilerle çalışmaktadır. Bu, saldırı senaryolarının önceden belirlenmesi veya etiketlenmiş verilere ihtiyaç duyulmaması anlamına gelmektedir. İHA'ların güvenliği ile ilgili veri toplama süreci genellikle karmaşık ve maliyetli olduğundan, gözetimsiz öğrenme yöntemleri önemli bir avantaj sağlamaktadır.
- Otomatik Kodlayıcı, normal İHA verilerinden özelliklerin otomatik olarak çıkarılmasını sağlamaktadır. Model, girdi verilerini sıkıştırırken önemli özellikleri öğrenir ve anormal verileri bu özelliklerle karşılaştırmaktadır. Bu sayede, anormallik tespiti için insan müdahalesine ihtiyaç duyulmadan, otomatik ve veriye dayalı bir yaklaşım kullanılabilmektedir.
- Otomatik Kodlayıcı, İHA sistemlerindeki değişikliklere ve yeni saldırı senaryolarına kolaylıkla adapte olabilmektedir. Yeni bir saldırı senaryosu ortaya çıktığında, modele yeni anormal veriler eklenerek veya mevcut model yeniden eğitilerek sisteme adapte edilebilmektedir. Bu, Otomatik Kodlayıcı'nın esneklik sağlayan bir yöntem olduğunu göstermektedir.

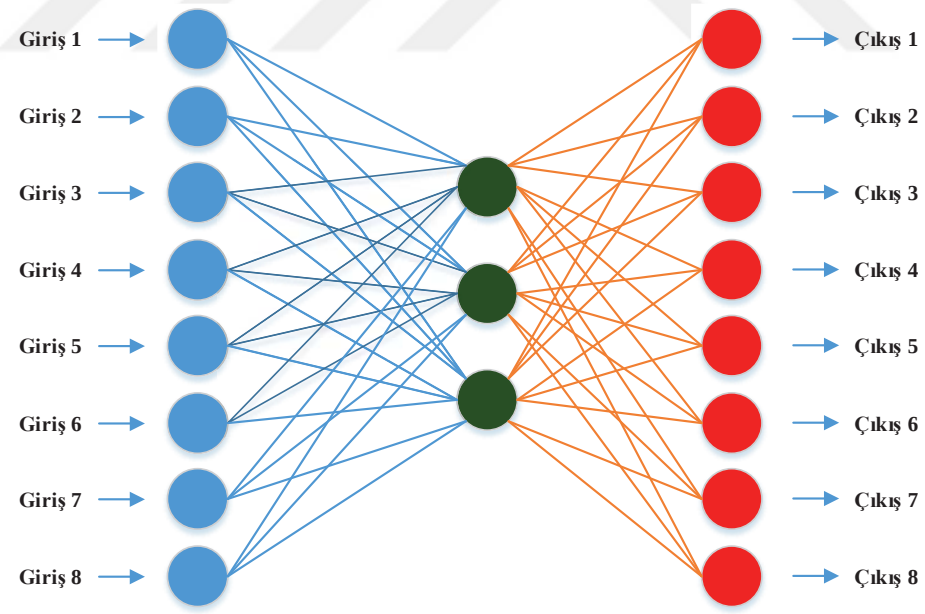
Otomatik Kodlayıcı, İHA'ların yapılan saldırılar veya anormallik durumları için anormallik tespiti konusunda etkili bir yöntemdir. Eğitim verileri kullanılarak Otomatik Kodlayıcı modeli eğitilir ve ardından test verileri üzerinde rekonstrüksiyon hataları hesaplanarak anormallik tespiti

yapılmaktadır. Otomatik Kodlayıcı'nın gözetimsiz öğrenme yeteneği, özellikleri otomatik olarak çıkarabilmesi ve adaptasyon yeteneği, İHA'larda anormallik tespiti için avantajlar sağlamaktadır.

Otomatik Kodlayıcı yöntemi, İHA'ların güvenliği için önemli bir araç olabilmektedir. Ancak, doğru eğitim verisi seçimi, modelin iyi ayarlanması ve optimize edilmesi gibi faktörlerin dikkate alınması önemlidir. Otomatik Kodlayıcı yönteminin kullanımıyla, İHA'lara karşı saldırıları veya anormallik durumlarını tespit etmek daha etkili ve güvenilir bir şekilde mümkün olabilmektedir.

Otomatik Kodlayıcı, denetimsiz öğrenme yoluyla girdisine çok yakın bir görüntü çıkarmak için tasarlanmış bir tür yapay sinir ağı olmaktadır. Otomatik kodlayıcı ve kod çözücü sinir ağlarından oluşmaktadır. Denklem 5.15'te Otomatik kodlayıcının giriş verisini önce kodlayarak düşük boyutlu z vektörüne dönüştürmesi, daha sonra bu vektörü tekrar orijinal boyutuna geri döndürmesi (x) matematiksel olarak ifade edilmektedir [39]. Karesel hata veya çapraz entropi gibi farklı kayıp fonksiyonları kullanılarak ölçülebilen yeniden oluşturma hatası, parametreleri optimize edilerek en aza indirmektedir. Şekil 5.32'de gösterilen yapı otomatik kodlayıcı, kodlama ve kod çözme katmanlarına sahiptir.

$$z = f(w_x + b)$$
$$x = g(w_z + B) \qquad (5.10)$$



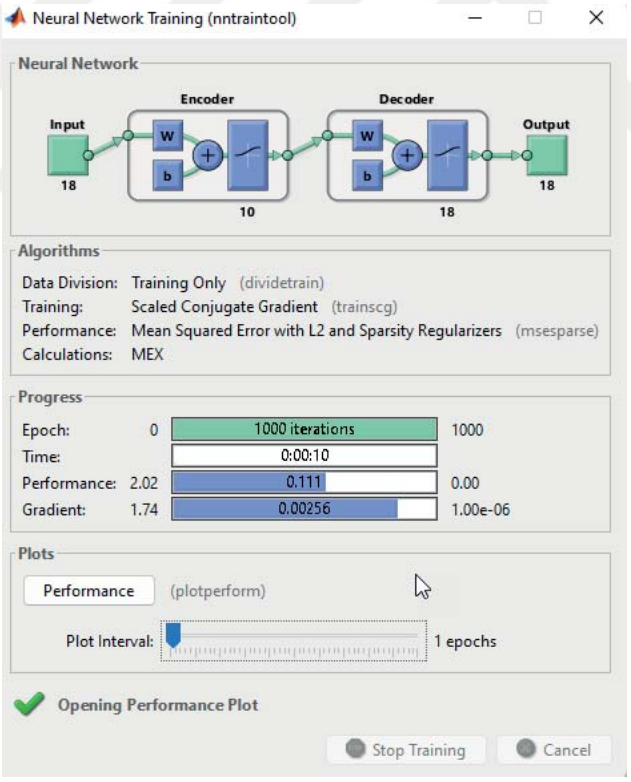
Şekil 5.32. Otomatik Kodlayıcı şematik gösterimi.

Veri işleme sürecinde, otomatik kodlayıcıya bağlı olarak çeşitli işlemler gerçekleştirilebilmektedir. İlk adım, verinin hazırlanmasıdır. Veri seti, uygun bir formatta ve gerektiğinde önişleme adımlarından geçirilerek kodlayıcıya beslenmektedir.

Kodlayıcı, veriyi sıkıştırılmış bir temsile dönüştürürken, önemli özellikleri belirlemek için özellik detektörleri kullanmaktadır. Bu özellik detektörleri, genellikle bir matris boyutunda temsil edilir ve belirli özelliklere duyarlıdırlar. Özellik detektörleri, giriş verisiyle eleman bazında çarpılarak özellik haritalarını oluşturmaktadır. Özellik haritaları, giriş verisinin boyutunu küçültür ve işlemeyi daha kolay ve daha hızlı hale getirmektedir.

Bu adımda, bazı veri özellikleri kaybolabilir, ancak verinin ana özellikleri korunmaktadır. Özellik haritaları, veri içerisindeki belirli özelliklerin nerede bulunduğunu algılamaya yardımcı olmaktadır. Bu özellik haritaları, veri üzerinde yapısal bilgileri koruyarak veri kaybını önlemektedir.

Şekil 5.33'te otomatik kodlayıcının Matlab programında gerçekleştirilen eğitim ara yüzü görülmektedir. Şekilde hem kullanılan eğitim ve performans fonksiyonları hem de durdurma kriterleri verilmektedir. Ağ mimarisine bakıldığında giriş boyutunun 18, enkoder katmanının 10, dekoder katmanı ve çıkış katmanının ise 18 nörondan oluştuğu görülmektedir. Eğitim süreci varsayılan iterasyon sayısına (1000) ulaşıldığı için tamamlanmıştır.

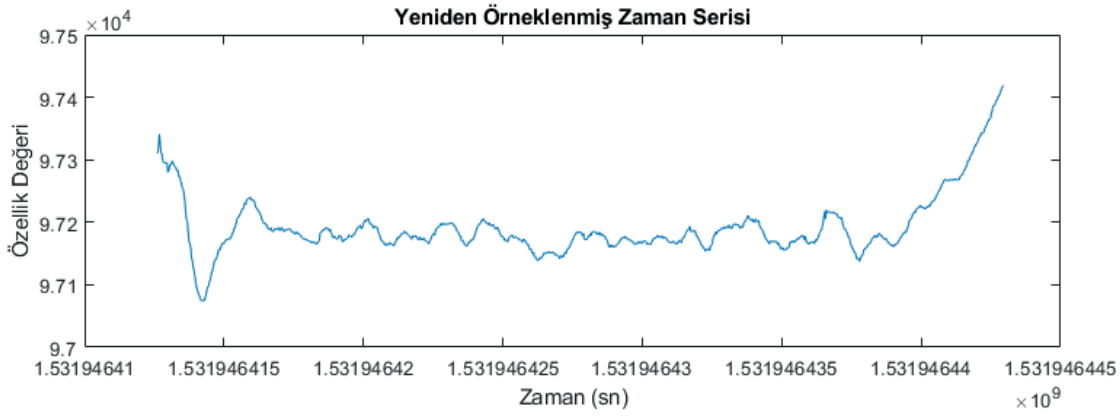


Şekil 5.33. Otomatik kodlayıcının eğitim süreci

5.6.1. Otomatik Kodlayıcı ile Motor Arızalarının Tespiti

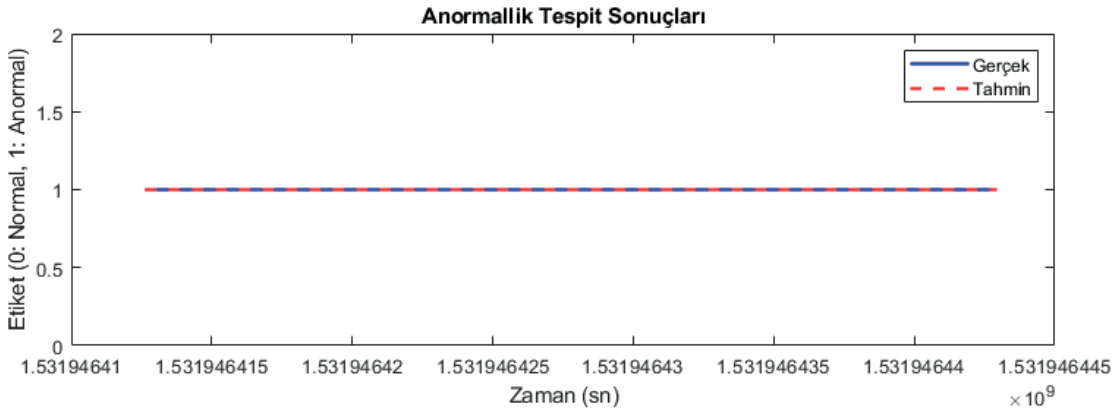
Bu bölümde, otomatik kodlayıcı modelinin motor arızası tespitinde elde edilen sonuçlar ayrıntılı bir şekilde sunulmuştur. Motor arızası tespiti testleri sonucunda, otomatik kodlayıcı

modelinin %100 başarı elde ettiği gözlemlenmiştir. Gerekli ön işleme adımları ve veri hazırlama süreçleri sonucunda elde edilen homojen veri yapısı, modelin motor arızalarını güvenilir bir şekilde ayırt etmesine olanak sağlamıştır. Şekil 5.34'de yer alan özellik zaman serisi, yeniden örnekleme ve interpolasyon işlemleri sonucu oluşturulan dengeli veri yapısını göstermektedir.



Şekil 5.34. Yeniden örneklenmiş motor arızası zaman serisi

Gerçek ve tahmin edilen sonuçların karşılaştırıldığı Şekil 5.35'de, otomatik kodlayıcı modelinin motor arızası tespitinde yüksek doğruluk sağladığını göstermektedir. Modelin tahminleri gerçek sonuçlarla büyük oranda uyumlu bir şekilde eşleşmektedir.



Şekil 5.35. Motor arızasına ait gerçek ve tahmin edilen otomatik kodlayıcı sınıflandırma sonuçları.

Performans metrikleri tablosu (Tablo 5.13), modelin hassasiyet, duyarlılık, F1 skoru ve doğruluk değerlerinin tamamının 1 olarak hesaplandığını ortaya koymaktadır. Bu sonuçlar, otomatik kodlayıcı modelin motor arızası tespitinde olağanüstü bir etkinlik ve güvenilirlik sergilediğini vurgulamaktadır.

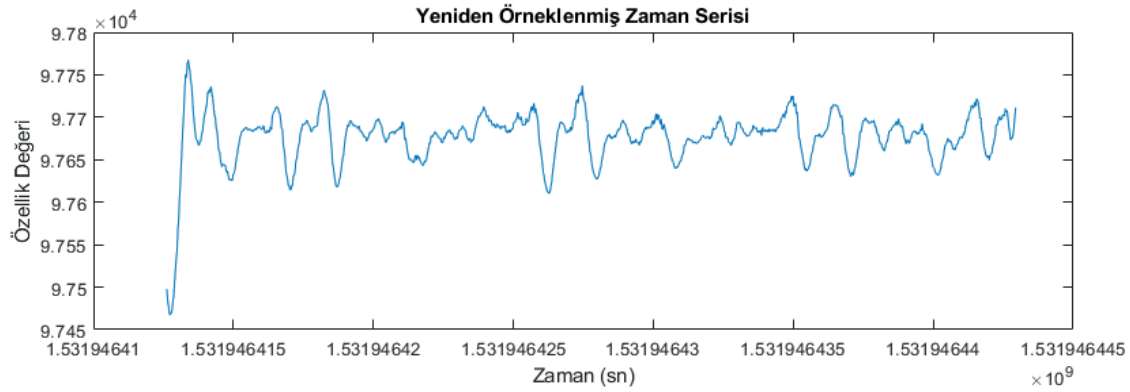
Otomatik kodlayıcı modelin motor arızası tespiti konusundaki yüksek performansı, havacılık endüstrisinin güvenliği açısından büyük bir öneme sahiptir. Modelin arıza tespiti sürecindeki etkinliği, endüstri uygulamalarında ciddi bir katkı sağlayabilecek potansiyele sahiptir.

Tablo 5.13. Motor arızası için otomatik kodlayıcı performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

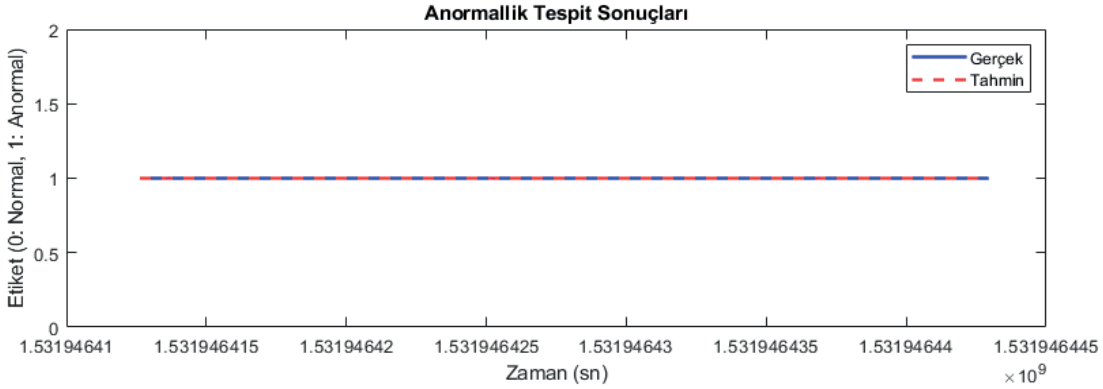
5.6.2. Otomatik Kodlayıcı ile Kanatçık Arızalarının Tespiti

Hava araçlarının kanatçık bölgelerindeki olası arızaların tespiti, uçuş güvenliği için kritik bir öneme sahiptir. Şekil 5.36'da yeniden örnekleme ve interpolasyon işlemleri sonucunda oluşturulan bir özellik zaman serisi verilmiştir. Oluşturulan homojen veri yapısı, modelin güvenilir ve dengeli sonuçlar üretmesine olanak sağlamaktadır.



Şekil 5.36. Yeniden örneklenmiş kanatçık arızası zaman serisi

Şekil 5.37'deki gerçek ve tahmin edilen sınıflandırma karşılaştırmasından, otomatik kodlayıcı modelinin kanatçık arızası tespitinde yüksek bir doğruluk elde ettiği anlaşılmaktadır. Modelin tahminleri, gerçek sonuçlarla büyük benzerlik göstermekte ve arıza tespitinde güvenilir bir araç olduğunu vurgulamaktadır. Kanatçık arızası anomali tespitinde kullanılan 8.000 adet arızalı verinin tamamını doğru olarak tahmin etmiştir.



Şekil 5.37. Kanatçık arızasına ait gerçek ve tahmin edilen otomatik kodlayıcı sınıflandırma sonuçları.

Performans metrikleri tablosu (Tablo 5.14), modelin hassasiyet, duyarlılık, F1 skoru ve doğruluk değerlerinin tamamının 1 olarak hesaplandığını göstermektedir. Bu sonuçlar, otomatik kodlayıcı modelin kanatçık arızası tespitinde etkili bir performans sergilediğini ve güvenilir sonuçlar ürettiğini ortaya koymaktadır.

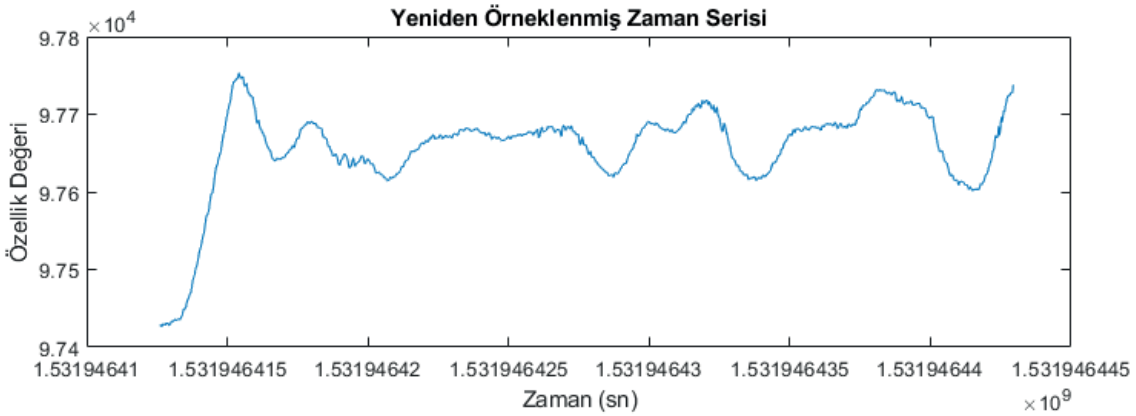
Otomatik kodlayıcı modelin kanatçık arızası tespiti konusundaki başarısı, havacılık endüstrisinin arıza tespit süreçlerini daha güvenilir ve verimli hale getirme potansiyelini yansıtmaktadır.

Tablo 5.14. Kanatçık arızası için otomatik kodlayıcı performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

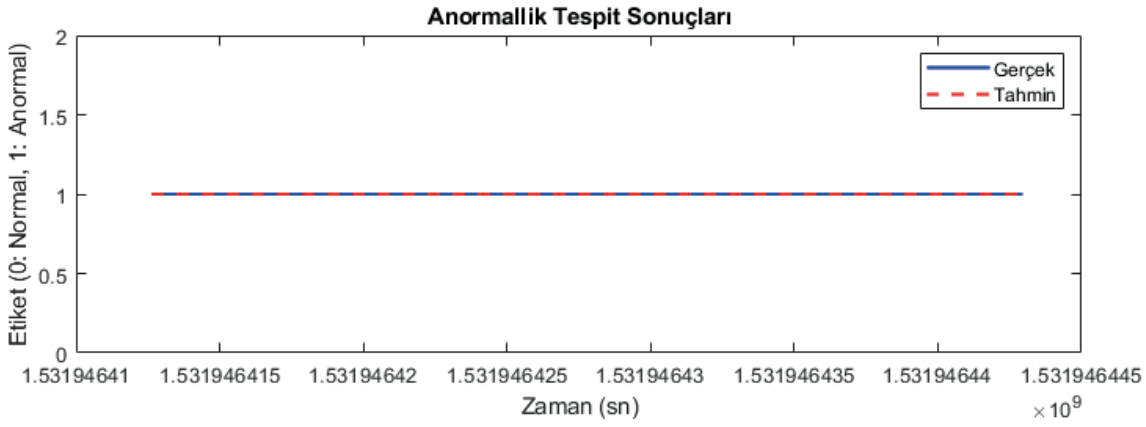
5.6.3. Otomatik Kodlayıcı ile Dümen Arızalarının Tespiti

Veri örnekleme ve interpolasyon süreçleri sonucu oluşturulan homojen özellik zaman serisi (Şekil 5.38), modelin veri setini dengeli bir yapıya getirdiğini göstermektedir. Bu yapı, modelin güvenilir ve etkili sonuçlar üretmesine olanak tanımaktadır.



Şekil 5.38. Yeniden örneklenmiş dümen arızası zaman serisi

Grafiksel karşılaştırma (Şekil 5.39), otomatik kodlayıcı modelinin dümen arızası tespitinde yüksek bir başarı elde ettiğini göstermektedir. Tahmin edilen sonuçlar, gerçek sonuçlarla büyük benzerlik göstermekte ve modelin arıza tespitinde güvenilir bir performans sergilediğini vurgulamaktadır. Dümen arızası anomali tespitinde kullanılan 4.000 adet arızalı verinin tamamını doğru olarak tahmin etmiştir.



Şekil 5.39. Dümen arızasına ait gerçek ve tahmin edilen otomatik kodlayıcı sınıflandırma sonuçları.

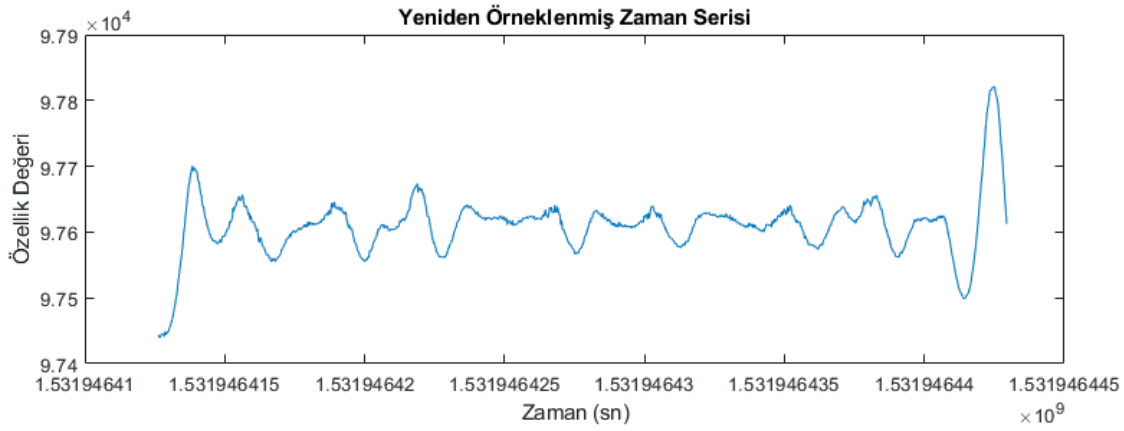
Performans metrikleri tablosu (Tablo 5.15), modelin hassasiyet, duyarlılık, F1 skoru ve doğruluk değerlerinin tamamının 1 olarak hesaplandığını göstermektedir. Bu sonuçlar, otomatik kodlayıcı modelin dümen arızası tespitinde yüksek bir etkinlik ve güvenilirlik sergilediğini göstermektedir. Otomatik kodlayıcı modelin dümen arızası tespiti konusundaki başarısı, uçuş güvenliğini artırma ve operasyonel süreçleri optimize etme hedefleri açısından önemli bir adımı temsil etmektedir.

Tablo 5.15. Dümen arızası için otomatik kodlayıcı performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

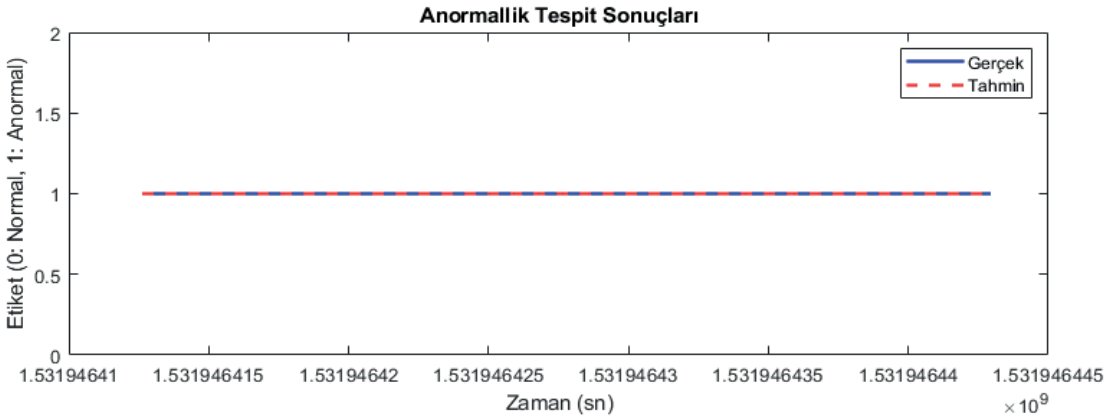
5.6.4. Otomatik Kodlayıcı ile Asansör Arızalarının Tespiti

Asansör sistemlerindeki olası arızaların erken tespiti, hava araçlarının güvenli uçuşunu sağlamak için temel bir gerekliliktir. Bu bölümde, otomatik kodlayıcı modelinin asansör arızası tespitindeki sonuçları detaylı bir şekilde analiz edilmiştir. Veri örnekleme ve interpolasyon süreçleri sonucu oluşturulan homojen özellik zaman serisi Şekil 5.40'da verilmiştir.



Şekil 5.40. Yeniden örneklenmiş asansör arızası zaman serisi

Grafiksel karşılaştırma (Şekil 5.41), otomatik kodlayıcı modelinin asansör arızası tespitinde yüksek bir başarı elde ettiğini göstermektedir. Modelin tahminleri gerçek sonuçlarla büyük oranda uyumlu bir şekilde eşleşmektedir, bu da modelin güvenilirliğini vurgulamaktadır. Asansör arızası anomali tespitinde kullanılan 2.000 adet arızalı verinin tamamı doğru olarak tahmin etmiştir. Şekil 5.41'ta gösterilmektedir.



Şekil 5.41. Asansör arızasına ait gerçek ve tahmin edilen otomatik kodlayıcı sınıflandırma sonuçları.

Performans metrikleri tablosu (Tablo 5.16), modelin hassasiyet, duyarlılık, F1 skoru ve doğruluk değerlerinin tamamının 1 olarak hesaplandığını göstermektedir. Bu sonuçlar, otomatik kodlayıcı modelin asansör arızası tespitinde yüksek bir performans ve güvenilirlik sergilediğini göstermektedir.

Otomatik kodlayıcı modelin asansör arızası tespitindeki başarısı, havacılık endüstrisinin operasyonel etkinliğini artırma ve güvenliği sağlama hedefleri açısından önemli bir gelişmeyi ifade etmektedir.

Tablo 5.16. Asansör arızası için otomatik kodlayıcı performans değerlendirmesi.

Performans Değerlendirme Metrikleri	Değeri
Doğruluk (Accuracy)	1
Hassasiyet (Precision)	1
Duyarlılık (Recall)	1
F1-Ölçüsü (F1-Score)	1

6. SONUÇLAR

Bu Tez çalışması, İHA'ların anormallik tespiti için geliştirilen yenilik tabanlı bir yöntemin etkinliğini incelemeyi amaçlamıştır. ALFA veri seti üzerinde gerçekleştirilen deneysel çalışma sonuçları, önerilen yöntemin geniş uygulama potansiyeli taşıdığını ortaya koymaktadır.

Veri setinin farklı boyutlarından kaynaklanan dengesizlikleri gidermek ve homojen bir yapı oluşturmak amacıyla interpolasyon yöntemi uygulandı. Ayrıca, veri setindeki özelliklerin ölçek farklılıklarını gidermek için z-skor normalizasyonu kullanıldı. Seçilen 18 ortak özelliğin diğer arıza türlerinde de etkili sonuçlar üretebilmesi, yöntemin genellemesini desteklemektedir.

Çalışmada OC-SVM, OC-RF, LOF ve Otomatik Kodlayıcı gibi farklı tek sınıflı sınıflandırma yöntemleri kullanıldı.

OC-SVM, OC-RF ve Otomatik Kodlayıcı yöntemleri %100 başarı oranıyla çalıştı. Bu yöntemlerin tümünde accuracy, precision, recall ve F1 skorları 1 olarak hesaplandı. Bu sonuçlar, güvenli uçuş verilerini eğitim için kullandığımızda bile yöntemlerin anormallikleri tespit etme konusundaki etkinliğini vurgulamaktadır.

LOF yöntemi, yüksek doğruluk oranına sahip olmakla birlikte bazı örneklerde hafif hatalar yapmıştır. Bu sonuç, LOF'un genel olarak etkili bir yöntem olduğunu gösterirken, özgün yapısı nedeniyle bazı örneklerde performansın düşebileceğini işaret etmektedir. Seçilen 18 ortak özelliğin farklı arıza türlerinde de etkili sonuçlar vermesi, yöntemin geniş bir uygulama alanına sahip olduğunu göstermektedir.

Gelecekteki çalışmalarda daha büyük veri setleri ve farklı özellik kombinasyonları kullanarak yöntemin genellemesi daha da test edilebilir. Ayrıca, derin öğrenme yöntemlerinin ve farklı veri ön işleme adımlarının etkisi daha kapsamlı şekillerde araştırılabilir.

Bu çalışma, ALFA veri seti üzerinde gerçekleştirilen yenilik tabanlı yaklaşımın, UAV'lerin anormallik tespitinde yüksek performans sağladığını göstermektedir. Seçilen özelliklerin ve yöntemlerin, güvenli uçuş verileri ile diğer arızaların tespitinde etkili sonuçlar verdiği kanıtlanmıştır.

Bu çalışma, havacılık endüstrisindeki güvenliği artırmak ve anormallikleri erken aşamada tespit etmek isteyen araştırmacılar ve profesyoneller için önemli bir kaynak olabilir. Genel bir değerlendirme yapmak için Tablo 6.1'de kullanılan sınıflandırıcıların performans ölçütleri her bir arıza tipi için bir arada verilmiştir.

Tablo 6.1. Genel performans değerlendirilmesi.

YÖNTEM	GÖSTERGE	Asansör	Kanatçık	Motor	Dümen
OC-SVM	Doğruluk	1	1	1	1
	Hassasiyet	1	1	1	1
	Duyarlılık	1	1	1	1
	F1-Skoru	1	1	1	1
LOF	Doğruluk	0.998	0.999	0.999	0.999
	Hassasiyet	1	1	1	1
	Duyarlılık	0.998	0.999	0.999	0.999
	F1-Skoru	0.998	0.999	0.999	0.999
OC-RF	Doğruluk	1	1	1	1
	Hassasiyet	1	1	1	1
	Duyarlılık	1	1	1	1
	F1-Skoru	1	1	1	1
Otomatik Kodlayıcı	Doğruluk	1	1	1	1
	Hassasiyet	1	1	1	1
	Duyarlılık	1	1	1	1
	F1-Skoru	1	1	1	1

Verilen sonuçlar ve performans metrikleri göz önüne alındığında, aşağıda arıza tespiti üzerinde yapılacak çalışmalar için bazı öneriler sunulmuştur:

- Veri Toplama: Daha fazla ve çeşitli arıza verileri toplamak, modelin genel performansını artırabilir. Bu, farklı koşullar altında daha fazla arıza senaryosunu kapsayan daha büyük bir veri kümesi oluşturmayı içerebilir.
- Veri Düzeltme: Veri düzeltme ve temizleme yöntemleri kullanarak, gürültülü veya eksik verileri eleme veya düzeltme işlemleri yapmak modelin performansını artırabilir.
- Özellik Mühendisliği: Daha iyi sonuçlar elde etmek için özellik mühendisliği yapılabilir. Bu, mevcut özelliklerin yanı sıra yeni özelliklerin de türetilmesini içerebilir. Arızaların belirli özelliklerini vurgulayan veya ayrıştıran yeni özellikler ekleyerek modelin öğrenme yeteneği geliştirilebilir.
- Model Parametre Ayarı: Modelin hiperparametrelerini ayarlamak, performansını artırmada önemli bir faktör olabilir. Farklı hiperparametre kombinasyonlarını deneyerek ve doğrulama seti üzerinde kapsamlı bir hiperparametre ayarlama süreci yürüterek daha iyi sonuçlar elde edebilirsiniz.
- Birleşik Modeller: Birden fazla modelin birleştirildiği birleşik sınıflandırma yöntemleri kullanarak daha güçlü bir arıza tespit sistemi oluşturabilirsiniz. Farklı modellerin çeşitliliği, genel performansı artırabilir ve daha güvenilir sonuçlar sağlayabilir.
- Güncel Tutma: Makine öğrenimi yöntemlerinde teknolojik ilerlemeler meydana gelebilir. Bu nedenle, sisteminizi güncel tutmak için yeni teknikleri ve algoritmaları takip etmek önemlidir. Yeni gelişmeleri gözlemlemek ve uygulamak, performansınızı artırabilir.

KAYNAKLAR

[1] "Türk Hava Kurumu -İHA," 2023. https://www.thk.org.tr/iha

[2] Önemi Y.V.E., (2019) İnsansız Hava Araçlarinin Savunma Sanayi Harcamasinda Yeri ve Önemi, *Avrasya Sos. ve Ekon. Araştırmaları Derg.*, 6(2), pp. 127–134,.

[3] Bernal A. S., Detection solution analysis for simplistic spoofing attacks in commercial mini and micro UAVs. 2016, [Online]. Available: https://core.ac.uk/download/pdf/83597546.pdf Erişim Tarihi 20.04.2023

[4] Sedjelmaci, H., Senouci S. M., Messous, M.A. (2016) How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?," in *2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6.

[5] Muniraj, D., Farhood, M. (2017) A framework for detection of sensor attacks on small unmanned aircraft systems," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 1189–1198. doi: 10.1109/ICUAS.2017.7991465.

[6] Zhu, H., Elfar, M., Pajic, M., Wang, Z. and Cummings, M. L. (2018) Human Augmentation of UAV Cyber-Attack Detection, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10916 LNAI, pp. 154–167. doi: 10.1007/978-3-319-91467-1_13.

[7] Solodov, A. Williams, A., Al Hanaei, S., and Goddard, B. (2018) Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities," *Secur. J.*, 31(1), pp. 305–324, doi: 10.1057/s41284-017-0102-5.

[8] Renyu, Z. Kiat, S. C., Kai, W. and Heng, Z. (2018) Spoofing Attack of Drone, in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 1239–1246. doi: 10.1109/CompComm.2018.8780865.

[9] Sedjelmaci, H., Senouci, S. M. and Ansari, N. (2018) A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks," *IEEE Trans. Syst. Man, Cybern. Syst.*, 48(9), pp. 1594–1606, doi: 10.1109/TSMC.2017.2681698.

[10] Whelan, J. Sangarapillai, T. Minawi, O. Almehmadi, A. and El-Khatib, K. (2020) Novelty-based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles. in *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Nov. pp. 23–28. doi: 10.1145/3416013.3426446.

[11] Rahman, M.A. Rahman, M. T. Kisacikoglu, M. T. and Akkaya, K. (2020) Intrusion Detection Systems-Enabled Power Electronics for Unmanned Aerial Vehicles. in *2020 IEEE CyberPELS (CyberPELS)*, pp. 1–5.

[12] Park, K. H., Park, E. Kim, H. K. (2021) Unsupervised Fault Detection on Unmanned Aerial Vehicles: Encoding and Thresholding Approach," *Sensors*, 21(6), 2208, doi: 10.3390/s21062208.

[13] Davidovich, B.. Nassi, B., and Elovici, Y. (2022) Towards the Detection of GPS Spoofing Attacks against Drones by Analyzing Camera's Video Stream," *Sensors*, 22(7) doi: 10.3390/s22072608.

[14] Chamola, V. Kotesh, P. Agarwal, A. Naren, Gupta, N. and Guizani, M. (2020) A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques," *Ad Hoc Networks*, vol. 111, 102324, 2021, doi: 10.1016/j.adhoc.2020.102324.

[15] Yiğit, E. Yazar, I. and Karakoç, T. H. İnsansız Hava Araçları (İHA)'nın Kapsamlı Sınıflandırması Ve Gelecek Perspektifi," *Sürdürülebilir Havacılık Araştırmaları Derg.*, vol. 3(1), pp. 10–19, 2018, doi: 10.23890/suhad.2018.0102.

[16] Uyar, E. (2019) İnsansız Hava Araçlarında GPS Aldatmacası Tespiti. Yayınlanmamış Yükseklisans tezi. Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2019. [Online]. Available: https://acikbilim.yok.gov.tr/handle/20.500.12812/296504

[17] Sentsov, A. A. Polyakov, V. B. and Gladkii, N. A. (2018) Electronic Methods to Protect Unmanned Aerial Vehicles from Seizing Control. *2018 Wave Electron. its Appl. Inf. Telecommun. Syst. WECONF 2018*, 2019, doi: 10.1109/WECONF.2018.8604463.

[18] He, D. Chan, S., and Guizani, M. (2017) "Communication Security of Unmanned Aerial Vehicles," *IEEE Wirel. Commun.*, 24(4), pp. 134–139, , doi: 10.1109/MWC.2016.1600073WC.

[19] Genç Y. M., Erciyes, E. (2020) Türkiye İnsansız Hava Araçları Dergisi İnsansız Hava Araçları (İHA) Tehditleri ve Güvenlik Yönetimi Threats of Unmanned Aerial Vehicles (UAV) and Security Management. 2(2), pp. 36–42, [Online]. Available: https://dergipark.org.tr/en/pub/tiha/issue/58203/783360

[20] Yahuza, M., Mohd Yamanı I.I. *et al.*, Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges. *IEEE Access*, vol. 9, pp. 57243–57270, 2021,

[21] Haider M., Ahmed, I. and Rawat, D. B., (2022) Cyber Threats and Cybersecurity Reassessed in UAV-assisted Cyber Physical Systems. in *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2022, pp. 222–227. doi: 10.1109/ICUFN55119.2022.9829584.

[22] Tunc C. and Hariri, S. (2022) Self-Protection for Unmanned Autonomous Vehicles (SP-UAV): Design Overview and Evaluation," in *2022 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C)*, pp. 128–132. doi: 10.1109/ACSOSC56246.2022.00046.

[23] Choudhary, G. Sharma, V. You, I., Yim, K., Chen, I.-R. and Cho, J.-H. (2018) Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey. in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 560–565. doi: 10.1109/IWCMC.2018.8450305.

[24] Tseng, C.-Y. Balasubramanyam, P., Ko, C. Limprasittiporn, R. Rowe, J. and Levitt, K. (2003) A specification-based intrusion detection system for AODV. in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pp. 125–134. doi: 10.1145/986858.986876.

[25] Borisovic. D. Dynamic Signature Inspection-Based Network Intrusion Detection," *Pat. US6279113B1*, 15(1), pp. 1–29, 1991.

[26] Patcha A., and Park, J.-M. (2007) An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Comput. Networks*, 51(12), pp. 3448–3470 doi: 10.1016/j.comnet.2007.02.001.

[27] Aydın, M. A. Zaim, A. H. and Ceylan, K. G. (2009) A hybrid intrusion detection system design for computer network security," *Comput. Electr. Eng.*, 35(3), pp. 517–526, doi: 10.1016/j.compeleceng.2008.12.005.

[28] Keipour A., Mousaei, M. and Scherer, S. (2021) ALFA: A dataset for UAV fault and anomaly detection. *Int.J.Rob. Res.*, 40(2–3), pp. 515–520,doi: 10.1177/0278364920966642.

[29] Keipour, A., Mousaei, M., Scherer, S. (2019) Automatic Real-time Anomaly Detection for Autonomous Aerial Vehicles. in *2019 International Conference on Robotics and Automation (ICRA)*, , pp. 5679–5685. doi: 10.1109/ICRA.2019.8794286.

[30] Kılınçer, İ. F. (2022) Saldırı tespit ve engelleme sistemleri için yapay zeka tabanlı yeni bir güvenlik modelinin oluşturulması Building a new artificial intelligence based security model for intrusion detection and prevention systems. [Online]. Available: https://akademik.yok.gov.tr/AkademikArama/view/searchResultviewListThesis.jsp

[31] Fatih, E. (2016) Kurumsal Bilgisayar Ağlarındaki Trafik Bilgisinin Akıllı Sistemler İle Sınıflandırılması. [Online]. Available: https://acikerisim.firat.edu.tr/xmlui/bitstream/handle/11508/20779/432832.pdf?sequence=1&isAllowed=y

[32] Yang, J. Awan, A. J., and Vall-Llosera, G. (2019) Support Vector Machines on Noisy Intermediate Scale Quantum Computers.. doi: 10.13140/RG.2.2.17956.63360.

[33] Muñoz, A., and Moguerza, J. M. (2004) One-class support vector machines and density estimation: The precise relation," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 3287, pp. 216–223, 2004, doi: 10.1007/978-3-540-30463-0_27.

[34] Muñoz-Marí, J., Bovolo, F., Gómez-Chova, L., Bruzzone, L., and Camp-Valls, G. (, 2010) Semisupervised one-class support vector machines for classification of remote sensing data. *IEEE Trans. Geosci. Remote Sens.*, 48(8), pp. 3188–3197, doi: 10.1109/TGRS.2010.2045764.

[35] Demidova, L., and Ivkina, M. (*2020*) Approach to Determining the Boundaries of the Search Range for the Number of Trees in the Random Forest Algorithm. *2020 9th Mediterr. Conf. Embed. Comput. MECO* pp. 8–11, doi: 10.1109/MECO49872.2020.9134342.

[36] Wai, T. H. Young, M. T., and Szpiro, A. A. Random Spatial Forests. 831697, pp. 1–25, 2020, [Online]. Available: http://arxiv.org/abs/2006.00150

[37] Alghushairy, O., Alsini, R., Soule, T., and Ma, X. (2020) A Review of Local Outlier Factor Algorithms for Outlier Detection in Big Data Streams. *Big Data Cogn. Comput.*, 5(1), p. 1, doi: 10.3390/bdcc5010001.

[38] Breunig, M. M., Kriegel, H.P., Ng, R. T., and Sander, J. (2000) "LOF," in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*, pp. 93–104. doi: 10.1145/342009.335388.

[39] Thomas J. M., and A. P. E., (2022) Bio-medical Image Denoising using Autoencoders," in *2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS)*,. pp. 1–6. doi: 10.1109/ICNGIS54955.2022.10079813.